JC20 Rec'd PCT/PTO 29 MAR 2002

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. § 371		Attorney Docket No. F40.12-0006
		U.S. Application No. 10/089646
INTERNATIONAL APPLICATION PCT/FR0/02715	INTERNATIONAL FILING DATE 09.29.2000	PRIORITY DATE CLAIMED 01.10.1999

TITLE OF INVENTION
SET OF PARTICULAR KEYS FOR PROVING AUTHENTICITY OF AN ENTITY OR THE INTEGRITY OF A MESSAGE

APPLICANT(S) FOR DO/EO/US
GIULLOU, Louis et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to begin national examination procedures (35 U.S.C. 371(f). The submission must include items (5), (6), (9) and (20) indicated below.
4. [X] The US has been elected by the expiration of the 19th month from the priority date (Article 31).
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [X] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [X] has been communicated by the International Bureau.
   c. [] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [X] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
   a. [X] is attached hereto.
   b. [] has been previously submitted under 35 U.S.C. 154(d)(4).
   c. [] is not required, as the application was filed in English
7. [X] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [] are attached hereto (required only if not transmitted by the International Bureau).
   b. [] have been transmitted by the International Bureau.
   c. [] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [X] have not been made and will not be made.
8. [] A translation of the amendment to the claims under PCT Article 19 (35 U.S.C. 372(c)(3)).
9. [X] An unexecuted oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 37(c)(5)).

Items 11. to 17. Below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and .198.
12. [] An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included.
13. [X] A **FIRST** preliminary amendment.
14. [] A **SECOND** or **SUBSEQUENT** preliminary amendment.
15. [] A substitute specification.
16. [] A change of power of attorney and/or address letter.
17. [] A second copy of the published international application under 35 U.S.C. 154(d)(4).
18. [] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
19. [X] Other items or information:
    a. [X] Three (3) sheets of drawings.
    b. [X] Abstract typed on a separate page.
    c. [X] File data sheet.

[redacted]

JC10 Rec'd PCT/PTO 29 MAR 2002

U.S. APPLICATION NO.	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
10/089646	PCT/FR00/02715	F40.12-0006

20. [X] The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492(A)(1)-(5)):		
Search Report has been prepared by the EPO or JPO.....$860.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) $690.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)).....$710.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO..... .....$1000.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4).....$ 100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$860	
Surcharge of **$130.00** for furnishing the oath or declaration later than [] 20 [] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$0	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	20 - 20 =	0	X 18	$0	
Independent claims	1- 3 =	0	X 80	$0	
MULTIPLE DEPENDENT CLAIM (S) (if applicable)			+ $270.00	$0	
TOTAL OF ABOVE CALCULATIONS			=	$860	
[] Applicant claims small entity status See 37 CFR 1 27. The fees indicated above are reduced by 1/2.			-	$0	
SUBTOTAL			=	$860	
Processing fee of $130.00 for furnishing the English translation later than [] 20 [] 30 months from the earliest claimed priority date (37 CFR 1.492(f))				$0	
TOTAL NATIONAL FEE			=	$860	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property.			+	$0	
TOTAL FEES ENCLOSED			=	$860	
				Amount to be: refunded	**$**
				charged	**$**

a. [X] A check in the amount of $860.00 to cover the above fees is enclosed.

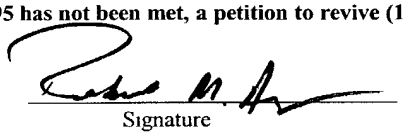
b. [] Please charge my Deposit Account No. **23-1123** in the amount of $ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Deposit Account No. **23-1123**. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (1.37(a) or (b)) must be filed and granted to restore the application to pending status.

Send all correspondence to:

Robert M. Angus
WESTMAN, CHAMPLIN & KELLY, P.A.
Suite 1600 - International Centre
900 Second Avenue South
Minneapolis, MN 55402-3319



Signature

Robert M. Angus
Reg. No. 24,383

[redacted]

10/089646
JC10 Rec'd PCT/PTO 29 MAR 2002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	: Louis Guillou et al.	
Appln. No.:		
Filed	: HEREWITH	Group Art Unit:
For	: SET OF PARTICULAR KEYS FOR PROVING AUTHENTICITY OF AN ENTITY OR THE INTEGRITY OF A MESSAGE	Examiner:
Docket No.:	F40.12-0006	

PRELIMINARY AMENDMENT

Box Non-Fee Amendment
Commissioner for Patents
Washington, D.C. 20231
Sir:

EXPRESS MAIL NO. EV049900720US
DATE OF DEPOSIT: March 29, 2002

Please amend the above-identified application as follows:

IN THE SPECIFICATION

On Page 1, before line 1 and after the title, please insert the following:

CROSS-REFERENCE TO RELATED APPLICATION

This application is a Section 371 National Stage Application of International Application No. PCT/FR00/02715 filed September 29, 2000 and published April 12, 2001 as WO 01/26278, not in English.

BACKGROUND OF THE INVENTION

On Page 3, between lines 28 and 29, please insert the following:

SUMMARY OF THE INVENTION

On page 9, line 36 delete the caption (line) and insert the following:

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. 1A-1D, 2A, 2B, 3A and 3B are graphs useful in explaining the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

IN THE CLAIMS

Please amend claims 1, 3-7, 9 and 11 as follows:

1.(Amended) A process intended to prove to a controller entity,

the authenticity of an entity and/or

the integrity of a message M associated with this entity;

said process implementing:

a public modulus n constituted by the product of f prime factors p_1, p_2 ... p_f, where f is greater than or equal to 2, or implementing the f prime factors;

m different whole base numbers g_1, g_2 ... g_m, where m is greater than or equal to 1, g_i being less than the f prime factors p_1, p_2 ... p_f;

m pairs of private Q_1, Q_2, ... Q_m and public G_1, G_2, ... G_m values, where m is greater than or equal to 1) or parameters derived from them;

said modulus and said private and public values being connected by relations of the type:

$$G_i.Q_i^v \equiv 1.\text{mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n$$

said public value G_i being the square g_i^2 of the base number, v denoting a public exponent of the form:

$$v=2^k$$

where k is a security parameter greater than 1;

the process according to the invention including the step of producing the f prime factors p_1, p_2 ... p_f and/or the m base numbers g_1, g_2 ... g_m in such a way that:

a) each of the equations:

$$x^v \equiv g_i^2 \text{mod } n$$

has solutions in x in the ring of the integers modulo n;

b) where $G_i \equiv Q_i^v \bmod n$, among the m numbers q_i obtained by raising Q_1 to the square modulo n, k-1 times of rank, one of them is different from $\pm g_i$ (in other words is nontrivial), and

where $G_i.Q_i^v \equiv 1 \bmod n$, among the m numbers q_i obtained by raising the inverse of Q_1 to the square modulo n, k-1 times of rank, one of them is different from $\pm g_i$ (in other words is nontrivial);

c) among the 2m equations:

$$x^2 \equiv g_i \bmod n$$
$$x^2 \equiv - g_i \bmod n$$

at least one of them has solutions in x in the ring of the integers modulo n;

the process for producing the f prime factors p_1, p_2 to p_f and/or the m base numbers g_1, g_2 to g_m includes the step of choosing :

the security parameter k
the m base numbers g_1, g_2 to g_m and/or the f prime factors p_1, p_2 to p_f.

Claim 2 remains unchanged.

3.(Amended) A process according to claim 1 such that the security parameter k is a small whole number, particularly less than 100.

4.(Amended) A process according to claim 1 such that the size of the modulus n is more than several hundred bits.

5.(Amended) A process according to claim 1 such that the f prime factors p_1, p_2 to p_f, have a size close to the size of the modulus n divided by the number f of factors.

6.(Amended) A process according to claim 1 such that to test the first condition, the compatibility of the numbers k, p, g is verified by implementing the algorithm of:

by h is denoted a number such that 2^h divides the rank of g relative to p and such that 2^{h+1} does not divide it,

h is computed from the Legendre symbol $(g|p)$ and from a number b equal to a 2^t-th primitive root of the unit in CG(p),

if $(g|p) = -1$ then $h = t$

if $(g|p) = +1$ with $t = 1$, then $h = 0$

if $(g|p) = +1$ with $t > 1$, then the key $\langle (p-1+2^t)/2^{t-1}, p\rangle$ is applied to G, a result w is thus obtained:

if $w = +g$, then $h = 0$

if $w = p-g$, then $h = +1$

otherwise, the computation sub-modulus below is applied, by initializing the variable c attributing to it the value b, then iterating the following steps for values of i from t-1 to 2:

step 1) the key $\langle 2^i, p\rangle$ is applied to w/g(modp),

if the result obtained is equal to +1, continue to step 2,

if the result obtained is equal to -1, the value i is attributed to h and w is replaced by w.c(modp),

step 2) c is replaced by c^2(modp),

the value of h sought is that obtained the last time the application of the key $\langle 2^i, p\rangle$, in accordance with step 1, produced a result equal to -1.

7.(Amended) A process according to claim 6 such that to test the second condition, a check is made that at least one set $\{\delta_{i.1} \ldots \delta_{i.f}\}$ is variable or nil.

Claim 8 remains unchanged.

9.(Amended) A process according to claim 1 such that to compute the f.m private components $Q_{i,j}$ of the private values Q_1, $Q_2 \ldots Q_m$ ($Q_{i,j} \equiv Q_i \bmod p_j$), where $G_i \equiv Q_i^v \bmod n$:

if $t = 1$ (i.e. if $p_j \equiv 3 \pmod 4$):

a number s_j is computed such that

$$s_j \equiv ((p_j+1)/4^k \pmod{(p_j-1)/2},$$

its key $\langle s_j, p_j \rangle$ is deduced,

the key $\langle s_j, p_j \rangle$ is applied to G_i,

so $w \equiv G_i^{sj} \pmod{p_j}$, and

the two possible values of $Q_{i,j}$ are w, $p_j - w$;

if $t = 2$ (i.e. if $p_j \equiv 5 \pmod 8$):

a number s_j is computed such that

$$s_j \equiv ((p_j+3)/8^k \pmod{(p_j-1)/4},$$

its key $\langle s_j, p_j \rangle$ is deduced,

the key $\langle s_j, p_j \rangle$ is applied to G_i,

so $w \equiv G_i^{sj} \pmod{p_j}$ and $w' \equiv w.z \pmod{p_j}$, and

the four possible values of $Q_{i,j}$ are w, $p_j - w$, w', $p_j - w'$,

if $t>2$ (i.e. if $p_j \equiv 2^t+1 \pmod{2^{t+1}}$) and if $h=0$ or if $h=1$,

a number s_j is computed such that

$$s_j \equiv ((p_j - 1 + 2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t},$$

its key $\langle s_j, p_j \rangle$ is deduced,

the key $\langle s_j, p_j \rangle$ is applied to G_i,

so $w \equiv G_i^{sj} \pmod{p_j}$,

the $2^{\min(k,t)}$ possible values of $Q_{i,j}$ are equal to the product of w by any one of the $2^{\min(k,t)}$ -th roots of the unit in $CG(p_j)$.

if $t>2$ (i.e. if $p_j \equiv 2^t+1 \pmod{2^{t+1}}$) and if $h>1$ and if $h+k \leq t+1$,

s_j is computed such that

$$s_j \equiv ((p_j - 1 + 2^t)/2^{t+1})^{k+h-1} \pmod{(p_j-1)/2^t},$$

its key $\langle s_j, p_j \rangle$ is deduced,

the key $\langle s_j, p_j \rangle$ is applied to the 2^{h-1}-th power G_i,

so w is thus obtained, and

the 2^k possible values of $Q_{i,j}$ belong to all the products of w by the 2^{k+h-1}-th primitive roots of the unit in $CG(p_j)$.

Claim 10 remains unchanged.

11.(Amended) A process according to claim 1, of allowing the f prime factors p_1, p_2 ... p_f or the m base numbers g_1, g_2 ... g_m to be produced:

said process being intended to prove to a controller entity,

the authenticity of an entity and/or

the integrity of a message M associated with this entity,

by means of m pairs of private Q_1, Q_2 .. Q_m and public G_1, G_2, ... G_m values, where m is greater than or equal to 1) or parameters derived from them, particularly by means of the private components $Q_{i,j}$:

said process implementing an entity called a witness by:

said witness entity having the f prime factors p_i and/or the parameters of the values of the Chinese remainders of the prime factors, and/or the public modulus n and/or the m private values Q_i and/or the f.m private components $Q_{i,j}$ of the private values Q_i and the public exponent v;

the witness computes commitments R in the ring of the integers modulo n: each commitment being computed:

either by performing operations of the type

$$R \equiv r^v \bmod n$$

where r is a random number such that $0<r<n$,

or

by performing operations of the type

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random number associated with the prime number p_i such that $0<r_i<p_i$, each r_i belonging to a collection of random numbers $\{r_1, r_2, \text{to } r_f\}$,

then by applying the method of Chinese remainders;

the witness receives one or more challenges d; each challenge d comprising m integers d_i hereinafter called

elementary challenges; the witness computes from each challenge d a response D,

either by performing operations of the type

$$D \equiv r.Q_1^{d1}.Q_2^{d2} \text{ to } Q_m^{dm} \bmod n$$

or

by performing operations of the type

$$D_i \equiv r_i.Q_{i,1}^{d1}.Q_{i,2}^{d2} \text{ to } Q_{i,m}^{dm} \bmod p_i$$

then by applying the method of Chinese remainders;

said process being such that there are as many responses D as challenges d and commitments R, each group of numbers R, d, D constituting a triplet denoted $\{R,d,D\}$.

Please add new claims 12-20 as follows:

12.(New) The process according to claim 2 such that the security parameter k is a small whole number, particularly less than 100.

13.(New) The process according to claim 2 such that the size of the modulus n is more than several hundred bits.

14.(new) A process according to claim 2 such that the f prime factors p_1, p_2 to p_f, have a size close to the size of the modulus n divided by the number f of factors.

15. A process according to claim 2 such that to test the first condition, the compatibility of the numbers k, p, g is verified by implementing the algorithm of:

by h is denoted a number such that 2^h divides the rank of g relative to p and such that 2^{h+1} does not divide it,

h is computed from the Legendre symbol $(g|p)$ and from a number b equal to a 2^t-th primitive root of the unit in CG(p),

if $(g|p) = -1$ then $h = t$

if $(g|p) = +1$ with $t = 1$, then $h = 0$

if $(g|p) = +1$ with $t > 1$, then the key $\langle (p-1+2^t)/2^{t-1}, p \rangle$ is applied to G, a result w is thus obtained:

if $w = +g$, then $h = 0$

if $w = p-g$, then $h = +1$

otherwise, the computation sub-modulus below is applied, by initializing the variable c attributing to it the value b, then iterating the following steps for values of i from t-1 to 2:

step 1) the key $\langle 2^i, p \rangle$ is applied to w/g(modp), and if the result obtained is equal to +1, continue to step 2,

if the result obtained is equal to -1, the value i is attributed to h and w is replaced by w.c(modp),

step 2) c is replaced by c^2(modp),

the value of h sought is that obtained the last time the application of the key $\langle 2^i, p \rangle$, in accordance with step 1, produced a result equal to -1.

16. A process according to claim 3 such that the size of the modulus n is more than several hundred bits.

17. A process according to claim 3 such that the f prime factors p_1, p_2 to p_f, have a size close to the size of the modulus n divided by the number f of factors.

18. A process according to claim 3 such that to test the first condition, the compatibility of the numbers k, p, g is verified by implementing the algorithm of:

by h is denoted a number such that 2^h divides the rank of g relative to p and such that 2^{h+1} does not divide it,

h is computed from the Legendre symbol $(g|p)$ and from a number b equal to a 2^t-th primitive root of the unit in CG(p),

if $(g|p) = -1$ then $h = t$

if $(g|p) = +1$ with $t = 1$, then $h = 0$

if $(g|p) = +1$ with $t > 1$, then the key $\langle (p-1+2^t)/2^{t-1}, p\rangle$ is applied to G, a result w is thus obtained:

if $w = +g$, then $h = 0$

if $w = p-g$, then $h = +1$

otherwise, the computation sub-modulus below is applied, by initializing the variable c attributing to it the value b, then iterating the following steps for values of i from t-1 to 2:

step 1) the key $\langle 2^i, p\rangle$ is applied to w/g(modp), and if the result obtained is equal to +1, continue to step 2,

if the result obtained is equal to -1, the value i is attributed to h and w is replaced by w.c(modp),

step 2) c is replaced by c^2(modp),

the value of h sought is that obtained the last time the application of the key $\langle 2^i, p\rangle$, in accordance with step 1, produced a result equal to -1.

19. A process according to claim 4 such that the f prime factors p_1, p_2 to p_f, have a size close to the size of the modulus n divided by the number f of factors.

20. A process according to claim 4 such that to test the first condition, the compatibility of the numbers k, p, g is verified by implementing the algorithm of:

by h is denoted a number such that 2^h divides the rank of g relative to p and such that 2^{h+1} does not divide it,

h is computed from the Legendre symbol $(g|p)$ and from a number b equal to a 2^t-th primitive root of the unit in CG(p),

if $(g|p) = -1$ then $h = t$

if $(g|p) = +1$ with $t = 1$, then $h = 0$

if $(g|p) = +1$ with $t > 1$, then the key $\langle (p-1+2^t)/2^{t-1}, p\rangle$ is applied to G, a result w is thus obtained:

if w = +g, then h = 0

if w = p-g, then h = +1

otherwise, the computation sub-modulus below is applied, by initializing the variable c attributing to it the value b, then iterating the following steps for values of i from t-1 to 2:

step 1) the key $\langle 2^i, p \rangle$ is applied to w/g(modp), and if the result obtained is equal to +1, continue to step 2,

if the result obtained is equal to -1, the value i is attributed to h and w is replaced by w.c(modp),

step 2) c is replaced by c^2(modp),

the value of h sought is that obtained the last time the application of the key $\langle 2^i, p \rangle$, in accordance with step 1, produced a result equal to -1.

REMARKS

Favorable action is respectfully requested.

The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: _____

Robert M. Angus, Reg. No. 24,383
Suite 1600 - International Centre
900 Second Avenue South
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

RMA:tas

MARKED-UP VERSION OF REPLACEMENT CLAIMS

1.(Amended) A process intended to prove to a controller entity,

——the authenticity of an entity and/or

——the integrity of a message M associated with this entity;

said process implementing:

——a public modulus n constituted by the product of f prime factors p_1, p_2 … p_f, where ~~(~~f ~~being~~is greater than or equal to 2~~)~~, or implementing the f prime factors;

——m different whole base numbers g_1, g_2 … g_m, where ~~(~~m ~~being~~is greater than or equal to 1~~)~~, g_i being less than the f prime factors p_1, p_2 … p_f;

m pairs of private Q_1, Q_2, … Q_m and public G_1, G_2, … G_m values, where ~~(~~m ~~being~~is greater than or equal to 1~~)~~ or parameters derived from them;

said modulus and said private and public values being connected by relations of the type:

$$G_i.Q_i^v \equiv 1.\text{mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n$$

said public value G_i being the square g_i^2 of the base number, v denoting a public exponent of the form:

$$v=2^k$$

where k is a security parameter greater than 1;

the process according to the invention including the step of producing the f prime factors p_1, p_2 … p_f and/or the m base numbers g_1, g_2 … g_m in such a way that: ~~the following conditions are met.~~

~~**First condition :**~~

~~According to the first condition,~~ a) each of the equations:

$$x^v \equiv g_i^2 \text{mod } n$$

has solutions in x in the ring of the integers modulo n~~.~~;

~~Second condition :~~

b) where $G_i \equiv Q_i^v \bmod n$, among the m numbers q_i obtained by raising Q_1 to the square modulo n, k-1 times of rank, one of them is different from $\pm g_i$ (in other words is nontrivial)~~.~~, and

where $G_i.Q_i^v \equiv 1 \bmod n$, among the m numbers q_i obtained by raising the inverse of Q_1 to the square modulo n, k-1 times of rank, one of them is different from $\pm g_i$ (in other words is nontrivial)~~.~~;

~~Third condition :~~

c) among the 2m equations:

$$x^2 \equiv g_i \bmod n \quad \text{~~(2)~~}$$
$$x^2 \equiv - g_i \bmod n \quad \text{~~(3)~~}$$

at least one of them has solutions in x in the ring of the integers modulo n;

the process ~~according to the invention~~ for producing the f prime factors p_1, p_2 to p_f and/or the m base numbers g_1, g_2 to g_m includes the step of choosing ~~firstly~~:

- the security parameter k
- the m base numbers g_1, g_2 to g_m and/or the f prime factors p_1, p_2 to p_f.

Claim 2 remains unchanged.

3.(Amended) A process according to ~~one of the~~ claims 1 ~~or 2~~ such that the security parameter k is a small whole number, particularly less than 100.

4.(Amended) A process according to ~~any one of~~ claims 1 ~~to 3~~ such that the size of the modulus n is more than several hundred bits.

5.(Amended) A process according to ~~any one of~~ claim~~s~~ 1 ~~to 4~~ such that the f prime factors p_1, p_2 to p_f, have a size close to the size of the modulus n divided by the number f of factors.

6.(Amended) A process according to ~~any one of~~ claim~~s~~ 1 ~~to 5~~ such that to test the first condition, the compatibility of the numbers k, p, g is verified by implementing the algorithm ~~given below~~of:

- by h is denoted a number such that 2^h divides the rank of g relative to p and such that 2^{h+1} does not divide it,
- h is computed from the Legendre symbol $(g|p)$ and from a number b equal to a 2^t-th primitive root of the unit in CG(p),
  - if $(g|p) = -1$ then $h = t$
  - if $(g|p) = +1$ with $t = 1$, then $h = 0$
  - if $(g|p) = +1$ with $t > 1$, then the key $\langle (p-1+2^t)/2^{t-1}, p \rangle$ is applied to G, a result w is thus obtained:
    - if $w = +g$, then $h = 0$
    - if $w = p-g$, then $h = +1$
    - otherwise, the computation sub-modulus below is applied, by initializing the variable c attributing to it the value b, then iterating the following steps for values of i from t-1 to 2:

step 1) ~~:~~ the key $\langle 2^i, p \rangle$ is applied to w/g(modp),

* if the result obtained is equal to +1, ~~go~~continue to step 2,
* if the result obtained is equal to -1, the value i is attributed to h and w is replaced by w.c(modp),

step 2) ~~:~~ c is replaced by c^2(modp),

the value of h sought is that obtained the last time the application of the key $\langle 2^i, p \rangle$, in accordance with step 1, produced a result equal to -1.

~~*(it may be recalled that*~~

~~*k, g, p are compatible when h>1 and when k+h>t+1,*~~

~~— k, g, p are compatible when h=0 or 1, whatever the value of k, or when h>1 and when k+h≤t+1).~~
~~(in said algorithm, the Legendre symbol and t have the sense defined in the description).~~

7. (Amended) A process according to claim 6 such that to test the second condition, a check is made that at least one set $\{\delta_{i.1} \ldots \delta_{i.f}\}$ is variable or nil~~,~~
~~(δ has the sense defined in the description)~~.

Claim 8 remains unchanged.

9. (Amended) A process according to ~~any one of~~ claims ~~1 to 8~~ such that to compute the f.m private components $Q_{i,j}$ of the private values $Q_1, Q_2 \ldots Q_m$ ($Q_{i,j} \equiv Q_i \bmod p_j$), where $G_i \equiv Q_i^v \bmod n$:

—if t = 1 (i.e. if $p_j \equiv 3 \pmod 4$):

- a number s_j is computed such that $s_j \equiv ((p_j+1)/4^k \pmod{(p_j-1)/2}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to G_i,
- ~~we thus have:~~ so $w \equiv G_i^{sj} \pmod{p_j}$, and
- the two possible values of $Q_{i,j}$ are w, $p_j - w$~~;~~

—if t = 2 (i.e. if $p_j \equiv 5 \pmod 8$):

- a number s_j is computed such that $s_j \equiv ((p_j+3)/8^k \pmod{(p_j-1)/4}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to G_i,
- ~~we thus have:~~ so $w \equiv G_i^{sj} \pmod{p_j}$ and $w' \equiv w.z \pmod{p_j}$, and
- the four possible values of $Q_{i,j}$ are w, $p_j - w$, w', $p_j - w'$,

~~(in said algorithm z has the sense defined in the description).~~

– if $t>2$ (i.e. if $p_j \equiv 2^t+1 \pmod{2^{t+1}}$) and if h=0 or if h=1,~

- a number s_j is computed such that $s_j \equiv ((p_j-1+2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to G_i,
- ~~we thus have:~~ so $w \equiv G_i^{sj} \pmod{p_j}$ ~~.~~,
- the $2^{\min(k,t)}$ possible values of $Q_{i,j}$ are equal to the product of w by any one of the $2^{\min(k,t)}$ -th roots of the unit in $CG(p_j)$.

—if $t>2$ (i.e. if $p_j \equiv 2^t+1 \pmod{2^{t+1}}$) and if $h>1$ and if $h+k \leq t+1$,

- s_j is computed such that $s_j \equiv ((p_j-1+2^t)/2^{t+1})^{k+h-1} \pmod{(p_j-1)/2^t}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to the 2^{h-1}-th power G_i,
- so w is thus obtained, and
- the 2^k possible values of $Q_{i,j}$ belong to all the products of w by the 2^{k+h-1}-th primitive roots of the unit in $CG(p_j)$.

Claim 10 remains unchanged.

11.(Amended) A process ~~applying the process,~~ according to ~~any one of the~~ claims ~~1 to 8~~, of allowing the f prime factors p_1, p_2 … p_f or the m base numbers g_1, g_2 … g_m to be produced:

said process being intended to prove to a controller entity,

– the authenticity of an entity and/or

– the integrity of a message M associated with this entity,

by means of m pairs of private Q_1, Q_2 … Q_m and public G_1, G_2, … G_m values, where ~~(~~m ~~being~~is greater than or equal to 1) or parameters derived from them, particularly by means of the private components $Q_{i,j}$:

said process implementing ~~according to the steps hereinafter~~ an entity called a witness by: ~~,~~

said witness entity having the f prime factors p_i and/or the

parameters of the values of the Chinese remainders of the prime factors, and/or the public modulus n and/or the m private values Q_i and/or the f.m private components $Q_{i,j}$ of the private values Q_i and the public exponent v;

——the witness computes commitments R in the ring of the integers modulo n: each commitment being computed:

- either by performing operations of the type

$$R \equiv r^v \bmod n$$

where r is a random number such that $0<r<n$,

- or
- by performing operations of the type

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random number associated with the prime number p_i such that $0<r_i<p_i$, each r_i belonging to a collection of random numbers $\{r_1, r_2, \text{to } r_f\}$,

- then by applying the method of Chinese remainders;

– the witness receives one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness computes from each challenge d a response D,

- either by performing operations of the type

$$D \equiv r.Q_1^{d1}.Q_2^{d2} \text{ to } Q_m^{dm} \bmod n$$

- or
- by performing operations of the type

$$D_i \equiv r_i.Q_{i,1}^{d1}.Q_{i,2}^{d2} \text{ to } Q_{i,m}^{dm} \bmod p_i$$

• • then by applying the method of Chinese remainders;

said process being such that there are as many responses D as challenges d and commitments R, each group of numbers R, d, D constituting a triplet denoted {R,d,D}.

10/089646

JC10 Rec'd PCT/PTO 29 MAR 2002

3/PRTS

SET OF SPECIAL KEYS INTENDED TO PROVE THE AUTHENTICITY OF AN ENTITY OR THE INTEGRITY OF A MESSAGE

The present invention relates to the technical field of the process, systems and devices intended to prove the authenticity of an entity and/or the integrity and/or the authenticity of a message.

The patent EP 0 311 470 B1 whose inventors are Louis Guillou and Jean-Jacques Quisquater describes such a process. Reference will be made hereinafter to their work by the terms: "GQ patent" or "GQ process". Hereinafter the terms "GQ2", "GQ2 invention" or "GQ2 technology" will sometimes be used to denote new developments in GQ technology which are subject to applications pending filed on the same day as the present application by France Telecom, TDF and the Mathrizk Company and having Louis Guillou and Jean-Jacques Quisquater as inventors. The characteristic features of these pending applications are recalled whenever it is necessary in the following description.

According to the GQ process, an entity called a "trusted authority" assigns an identity to each entity called a "witness" and computes its RSA signature: during a customizing process, the trusted authority gives the witness an identity and signature. Thereafter, the witness states: "*Here is my identity; I know its RSA*

signature." The witness proves without revealing it that he knows the RSA signature of his identity. By means of the RSA public verification key distributed by the trusted authority, an entity called a "controller" verifies without obtaining knowledge thereof that the RSA signature corresponds to the declared identity. The mechanisms using the GQ process operate "without transfer of knowledge". According to the GQ process, the witness does not know the RSA private key with which the trusted authority signs a large number of identities.

The GQ technology previously described uses RSA technology. But if RSA technology truly depends on the factorization of the modulus n, this dependence is not an equivalence, far from it, as is shown by the so-called "multiplicative" attacks against the different digital signature standards implementing RSA technology.

The objective of GQ2 technology is twofold: on the one hand, to improve performance relative to RSA technology; on the other hand, to avert the problems inherent in RSA technology. Knowledge of the private GQ2 private key is equivalent to knowledge of the factorization of modulus n. Any attack at the level of the GQ2 triplets goes back to the factorization of modulus n: this time there is equivalence. With GQ2 technology, the work load is reduced, both for the entity which signs or which authenticates itself and for the one that controls. By making better use of the factorization problem, both in security and in performance, GQ2 technology avoids the drawbacks presented by RSA technology.

The GQ process implements modulo computations of numbers of 512 bits or more. These computations relate to numbers having approximately the same size raised to powers of about $2^{16} + 1$. Existing microelectronic infrastructures, particularly in the field of bank cards, use monolithic self-programmable microprocessors

without arithmetical coprocessors. The work load associated with the multiple arithmetical operations involved in processes like the GQ process leads to computation times which in some cases prove to be disadvantageous for consumers using bank cards to pay for their purchases. It is recalled here, that in seeking to increase the security of payment cards, the banking authorities have raised a problem which is particularly difficult to resolve. Indeed two apparently contradictory questions have to be resolved: increase security by using increasingly lengthy and distinct keys for each card while preventing the work load from leading to excessive computation times for users. This problem becomes especially acute insofar as, additionally, the existing infrastructure and existing microprocessor components should be taken into account.

GQ2 technology brings a solution to this problem while tightening security.

GQ2 technology implements prime factors having particular properties. Different technologies exist to produce these prime factors. The subject of the present invention is a process making it possible to produce prime factors of this kind systematically. It also relates to the application which can be made of them more particularly in implementing the GQ2 technology. It is stressed here and now that these particular prime factors and the process allowing them to be obtained can be applied outside the field of GQ2 technology.

The invention applies to a process intended to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity.

Such a process implements:

- a public modulus n constituted by the product of f prime factors p_1, p_2 ... p_f (f being greater than or equal to 2) or implementing the f prime factors,

- m different whole base numbers g_1, g_2 ... g_m (m being greater than or equal to 1), g_i being less than the f prime factors p_1, p_2 ... p_f

- m pairs of private Q_1, Q_2, ... Q_m and public G_1, G_2, ... G_m values (m being greater than or equal to 1) or parameters derived from them.

Said modulus and said private and public values are connected by relations of the type:

$$G_i.Q_i^v \equiv 1.\text{mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n$$

said public value G_i being the square g_i^2 of the base number, v denoting a public exponent of the form:

$$v=2^k$$

where k is a security parameter greater than 1.

The process according to the invention includes the step of producing the f prime factors p_1, p_2 ... p_f and/or the m base numbers g_1, g_2 ... g_m in such a way that the following conditions are met.

First condition:

According to the first condition, each of the equations:

$$X^v \equiv g_1^2 \text{mod } n \quad (1)$$

has solutions in x in the ring of integers modulo n.

Second condition:

According to the second condition, where $G_i \equiv Q_i^v$ mod n, among the m numbers q_1 obtained by raising Q_1 to the square modulo n, k-1 times of rank, one of them is different by $\pm g_i$ (in other words is nontrivial).

According to the second condition, where $G_i.Q_i^v \equiv 1.\text{mod } n$, among the m numbers q_1 obtained by raising the inverse of Q_1 modulo n to the square modulo n, k-1 times of rank, one of them is different by $\pm g_i$ (in other words is nontrivial).

It is hereby stated that according to a common notation $\pm g_i$ represents the numbers g_i and $n-g_i$.

Third condition:

According to the third condition, among the 2m equations:

$$X^2 \equiv g_i \bmod n \quad (2)$$
$$X^2 \equiv - g_i \bmod n \quad (3)$$

at least one of them has solutions in x in the ring of integers modulo n.

The process according to the invention for producing the f prime factors p_1, p_2 … p_f and/or the m base numbers g_1, g_2 … g_m includes the step of choosing firstly:

- the security parameter k
- the m base numbers g_1, g_2 … g_m and/or the f prime factors p_1, p_2 … p_f, according to whether it is a matter of producing the f prime factors p_1, p_2 … p_f, or the m base numbers g_1, g_2 … g_m.

Preferably, the m base numbers g_1, g_2 … g_m are chosen at least partly among the first whole numbers.

Preferably, the security parameter k is a small whole number, particularly less than 100.

Preferably, the size of the modulus n is larger than several hundred bits.

Preferably, the f prime factors p_1, p_2 … p_f, have a size close to the size of the modulus n divided by the number f of factors.

To test the first condition, the compatibility of the numbers k, p, g is verified by implementing the algorithm given below, where h denotes a number such that 2^h divides the rank of g relative to p and such that 2^{h+1} does not divide it. h is computed from the Legendre symbol $(g|p)$ and from a number b equal to a 2^t-th primitive root of the unit in CG(p), where the Legendre symbol $(g_i|p_j)$ and t have the sense defined hereinafter in the description.

Here are the steps of this algorithm:

- if $(g|p) = -1$ then $h = t$
- if $(g|p) = +1$ with $t = 1$, then $h = 0$
- if $(g|p) = +1$ with $t > 1$, the procedure is as follows.

The key $\langle (p-1+2^l)/2^{t+1}, p\rangle$ is applied to G, a result w is thus obtained:

- if $w = +g$, then $h = 0$
- if $w = p-g$, then $h = +1$.

If w is different from +g or from p-g (in this case t is greater than 2), a computation sub-modulus is applied. The variable c is initialised attributing to it the value b, then the following steps of the computation sub-modulus are iterated for values of i running from t-1 to 2:

Step 1: the key $\langle 2^i, p\rangle$ is applied to w/g(modp),

* if the result obtained is equal to +1, go to step 2,

* if the result obtained is equal to +1, the value i is attributed to h and w is replaced by w.c(modp),

Step 2: c is replaced by c^2(modp),

The value of h sought is that obtained the last time the application of the key $\langle 2^i, p\rangle$, in accordance with step 1, produced a result equal to -1.

It may be remembered that:

- k, g, p are incompatible when h>1 and when k+h>t+1,

- k, g, p are compatible when h=0 or 1, whatever the value of k, or when h>1 and when $k+h \leq t+1$.

To test the second condition, a check is made that at least one set $\{\delta_{i,1} \ldots \delta_{i,f}\}$ is variable or nil, (δ has the sense defined hereinafter in the description).

To test the third condition, a check is made that there is a base number g_i from g_1 to g_m such that the f Legendre symbols $(g_i|p_1)$ to $(g_i|p_f)$ are all equal to +1 or else the Legendre symbols $(-g_i|p_1)$ to $(-g_i|p_f)$ are all equal to +1.

To compute the f.m private components $Q_{i,j}$ of the private values $Q_1, Q_2 \ldots Q_m$ ($Q_{i,j} \equiv Q_i \bmod p_j$), where $G_i \equiv Q_i^v \bmod n$, the procedure is as follows, distinguishing the cases according to the values of t.

Where t = 1 (i.e. if $p_j \equiv 3 \pmod 4$).

- a number s_j is computed such that $s_j \equiv ((p_j+1)/4^k \pmod{(p_j-1)/2}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to G_i,
- we thus have: $w \equiv G_i^{sj} \pmod{p_j}$.

The two possible values of $Q_{i,j}$ are w, $p_j - w$.

Where t = 2 (i.e. if $p_j \equiv 5 \pmod 8$).

- a number s_j is computed such that $s_j \equiv ((p_j+3)/8^k \pmod{(p_j-1)/4}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to G_i,
- we thus have: $w \equiv G_i^{sj} \pmod{p_j}$ and $w' \equiv w.z \pmod{p_j}$,

where z has the sense defined hereinafter in the description.

The four possible values of $Q_{i,j}$ are w, $p_j - w$, w', $p_j - w'$.

Where t>2 (i.e. if $p_j \equiv 2^t+1 \pmod{2^{t+1}}$) with h=0 or with h=1,

- a number s_j is computed such that $s_j \equiv ((p_j-1+2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t}$,

- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to G_i,
- we thus have: $w \equiv G_i^{sj} (\mathrm{mod} p_j)$.

The $2^{\min(k,t)}$ possible values of $Q_{i,j}$ are equal to the product of w by any one of the $2^{\min(k,t)}$ -th roots of the unit in $CG(p_j)$.

- where $t>2$ (i.e. if $p_j \equiv 2^t+1 (\mathrm{mod} 2^{t+1})$) with $h>1$ and with $h+k \leq t+1$,

- s_j is computed such that $s_j \equiv ((p_j-1+2^t)/2^{t+1})^{k+h-1} (\mathrm{mod}(p_j-1)/2^t)$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to the 2^{h1}-th power G_i,
- w is thus obtained,

The 2^k possible values of $Q_{i,j}$ belong to all the products of w by the 2^{k+h-1}-th primitive roots of the unit in $CG(p_j)$.

To compute the private components $Q_{i,j}$ where $G_i.Q_i^v \equiv 1.\mathrm{mod}\ n$, s_j is replaced by $((p_j-1)/2^t) - s_j$ in the key $\langle s_j, p_j \rangle$.

The invention also relates to a process applying the method allowing the f prime factors p_1, p_2 ... p_f or the m base numbers g_1, g_2 ... g_m to be produced.

Said process is intended to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message M associated with this entity,

by means of m pairs of private Q_1, Q_2 ... Q_m and public G_1, G_2, ... G_m values (m being greater than or equal to 1) or parameters derived from them, particularly by means of the private components $Q_{i,j}$.

Said process implements according to the steps below an entity called a witness.

Said witness entity has the f prime factors p_i and/or the parameters of the Chinese remainders of the

prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m private components $Q_{i,j}$ of the private values Q_i and the public exponent.

The witness computes commitments R in the ring of integers modulo n. Each commitment is computed:

- either by performing operations of the type

$$R \equiv r^v \bmod n$$

where r is a random number such that $0<r<n$,

- or by applying the method of Chinese remainders after performing operations of the type

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random number associated with the prime number p_i such that $0<r_i<p_i$, each r_i belonging to a collection of random numbers $\{r_1, r_2, \text{to } r_f\}$.

The witness receives one or more challenges d. Each challenge d comprising m integers d_i hereinafter called elementary challenges. The witness computes from each challenge d a response D,

- either by performing operations of the type

$$D \equiv r.Q_1^{d1}.Q_2^{d2} \text{ to } Q_m^{dm} \bmod n$$

- or by applying the method of Chinese remainders after performing operations of the type

$$D_i \equiv r_i.Q_{i,1}^{d1}.Q_{i,2}^{d2} \ldots Q_{i,m}^{dm} \bmod p_i$$

Said process is such that there are as many responses D as challenges d and commitments R. Each group of numbers R, d, D constitutes a triplet denoted $\{R,d,D\}$.

Description

The goal of GQ technology is the dynamic authentication of entities and messages and the digital signature of messages. It is technology "without transfer of knowledge". One entity proves: it knows one or more private numbers. Another entity controls: it knows the corresponding public number or numbers. The proving entity wishes to convince the controlling entity without revealing the private number or numbers, so as to be able to use them as many times as necessary.

Each GQ pattern is based on a public modulus composed of large secret prime numbers. A public exponent v and a public modulus n together form a verification key $\langle v, n \rangle$ signifying "raise to the power v modulus n" and implementation by means of one or more generic equations, all of the same direct type: $G \equiv Q^v \pmod{n}$ or the reverse: $GxQ^v \equiv 1 \pmod{n}$. The type has an effect on the operation of computations within the controlling entity, not within the proving entity; in fact the security analyses confuse the two types. Each generic equation links a public number G and a private number Q together forming a pair of numbers $\{G,Q\}$. To sum up, each GQ pattern implements one or more pairs of numbers $\{G,Q\}$ for the same key $\langle v, n \rangle$.

A conventional version of GQ patterns, here called GQ1, uses an RSA digital signature pattern. The verification key $\langle v, n \rangle$ is then an RSA public key where the uneven v exponent is preferably a prime number. Each GQ1 pattern generally uses a single pair of numbers $\{G,Q\}$: the public number G is deduced from identification data according to a format mechanism which is an integral part of the RSA digital signature pattern. The private number Q or else its inverse modulo n is an RSA signature of identification data. The proving entity demonstrates knowledge of an RSA signature from its own identification data and this proof does not reveal the

signature which therefore remains secret so as to be used as many times as necessary.

GQ1 patterns usually apply to two key levels: the RSA signature private key is reserved for an authority accrediting entities distinguishing themselves from each other via identification data. It is said that such a pattern is "identity based". Thus, a chip card issuer uses his RSA private key when issuing each card in order to compute a private number Q which it inscribes as a diversified private key in the card; or else, a customer on a computer network uses his RSA private key whenever logging on in order to compute a private number Q which will be the customer's ephemeral private key during the session. The proving entities, chip cards or customers logged on, know an RSA signature of their identification data; they do not know the RSA private key which, in the hierarchy of keys, is at the level immediately above. However a dynamic authentication of entities by GQ1 with a 768 bit modulus at the level of an authority requires approximately the same work load as a dynamic authentication of entities by RSA with a 512 bit modulus with three prime factors at the level of each entity, which allows the proving entity to use the technique of Chinese remainders by computing a result modulo each of the prime factors before computing a result modulo the product.

However, the hierarchy of keys between an authority and the accredited entities is not mandatory. GQ1 may be used with a modulus particular to the proving entity, which allows the technique of Chinese remainders to be used to reduce the work loads of the proving entity, which does not fundamentally change the work load of the controlling entity, apart from the fact that a modulus at proving entity level may be shorter than a modulus at authority level, for example 512 bits compared with 768 bits.

When the entity knows the prime factors of its own modulus, why use a digital signature RSA pattern?

Another version of GQ patterns, here called elementary GQ2 uses directly the problem of the factorization of a modulus n. In this context, "directly" signifies "without using the RSA signature". The purpose of GQ2 is in fact to reduce the work loads, not only of the proving entity but also of the controlling entity. The proving entity demonstrates knowledge of a decomposition of its own modulus and this proof does not reveal the decomposition which therefore remains secret to be used as many times as needed. The security of the GQ2 protocol is equivalent to the factorization of the modulus.

Each proving entity has its own modulus n. Each GQ2 pattern implements a parameter k, a small number larger than 1 fixing a public exponent $v=2^k$, and one or more pairs of numbers $\{G_1,Q_1\}$ to $\{G_m,Q_m\}$. Each public number G_1 is the square of a small number g_1 larger than 1 and called a "base number". All the proving entities may use the same public number or numbers G_1 to G_m. The factorization of the modulus n and the private number or numbers Q_1 to Q_m are then at the same level in the hierarchy of keys. Each set of GQ2 elementary keys is defined by two necessary and sufficient conditions.

- For each base number, neither of the two equations $x^2 \equiv \pm g_i \pmod{n}$ has a solution in x in the ring of the integers modulo n, i.e. the numbers $\pm g_i$ are two non-quadratic residues modulo n.

- For each base number, the equation $x^v \equiv g_1^2 \pmod{n}$ where $v = 2^k$ has solutions in x in the ring of the integers modulo n. The private number Q_1 or its inverse modulo n is either of these solutions.

Given the second condition, for the numbers $\pm g_i$ to be two non-quadratic residues modulo n, the modulus n must comprise at least two prime factors congruent with

3 (mod 4) relative to which the g_1 Legendre symbol differs. Consequently, any modulus composed of prime factors none or one of which is congruent with 3 (mod 4) does not allow a set of GQ2 elementary keys to be established, which favours prime factors congruent with 3 (mod 4). Drawing at random large prime numbers, about half of them prove to be congruent with 3 (mod 4) and half with 1 (mod 4). Therefore, many RSA moduli in use do not allow sets of elementary GQ2 keys to be established.

We introduce here the sets of GQ2 generalized keys use to overcome this limitation so as to be able to use GQ2 techniques with any modulus, in particular any RSA modulus; they are based on two necessary and sufficient principles.

The first principle reproduces the second GQ2 elementary condition.

For each base number g_1 to g_m, the equation $x^v \equiv g_i^2 \pmod{n}$ where $v=2^k$ has solutions in x in the ring of the integers modulo n.

Because the private number Q_1 or else its inverse modulo n is a solution to the equation, $k-1$ successive squares modulo n, convert it into a number q_i which is a square root of G_i in the ring of the integers modulo n. According to whether the number q_i is equal to one of the two numbers g_i or $n-g_i$, or different from the two numbers g_1 and $n-g_i$, we say that it is trivial or nontrivial. When a number q_i is nontrivial, n which divides $q_i^2-g_i^2$ divides neither q_i-g_i nor q_i+g_i. Any nontrivial number q_i therefore reveals a decomposition of the modulus n.

$$n=\mathrm{pgcd}(n,q_i-g_i)\times\mathrm{pgcd}(n,q_i+g_i)$$

The second principle broadens the first GQ2 elementary condition.

Among the numbers q_i to q_m at least one number q_i is nontrivial.

Let us note that if a number q_i exists when the numbers $\pm g_1$ are two non-quadratic residues in the ring of the integers modulo n, the number q_i is manifestly nontrivial. So, the sets of elementary GQ2 keys are fully part of the sets of GQ2 keys in general use which allow any modulus to be used, i.e. any composition of large prime numbers congruent irrespectively with 3 or with 1 (mod 4) at least two of which are distinct. On the other hand, many sets of GQ2 keys in general use are not sets of GQ2 elementary keys. Each set of GQ2 keys in general use is in one of the two following cases.

- When the 2xm numbers $\pm g_i$ to $\pm g_m$ are all non-quadratic residues, it is a set of GQ2 elementary keys.

- When among the 2xm numbers $\pm g_1$ to $\pm g_m$, there is at least one quadratic residue, it is not a set of GQ2 elementary keys; it is what we call here a set of GQ2 complementary keys.

The present invention relates to sets of GQ2 complementary keys, by definition, those sets of GQ2 keys in general use which are not elementary. Apart from the two previous principles, a set of this kind must satisfy a third principle.

- Among the 2xm numbers $\pm g_i$ to $\pm g_m$, there is at least one quadratic residue. To apprehend the problem and to understand the solution that we are providing for it, i.e. the invention, let us firstly analyse the decomposition of the modulus n revealed by a nontrivial number q, then let us remind ourselves of the technique of Chinese remainders, then, the notion of rank in a Galois field CG(p); then, let us study the functions of "raise to square" in CG(p) and "take a square root" of a quadratic residue in CG(p); lastly, let us analyse the applicability of the three principles stated above.

Analysis of the decompositions of the modulus- Just as the modulus n decomposes into f prime factors p_1 to p_f, the ring of the integers modulo n decomposes into f Galois fields CG(p_1) to CG(p_f). In each field, there are two square roots of the unit, namely ±1. In the ring, there are therefore 2^f square roots of the unit. Each private number Q_1 to Q_m defines a number $\Delta_i = q_1/g_1 \pmod n$ which is one of these 2^f square roots of the unit in the ring: in other words, n divides Δ_i^2-1.

- When q_i is trivial, i.e. $\Delta_i = \pm 1$, n divides Δ_i-1 or else Δ_i+1 and therefore Δ_i does not reveal any decomposition of modulus n.

- When q_i is nontrivial, i.e. $\Delta_i \neq \pm 1$, n divides neither Δ_i-1 nor Δ_i+1 and therefore Δ_i reveals a decomposition, $n=\text{pgcd}(n,\Delta_i-1)\text{X}\text{pgcd}(n,\Delta_i+1)$, resulting from the value of Δ_i in each field: the prime factor or factors dividing Δ_i-1 on the one hand, it or they dividing Δ_i+1 on the other.

Let us examine the multiplicative composition rules of the numbers q. Two numbers $\{q_1,q_2\}$ give one composite number $q_1 \times q_2 \pmod n$.

- when q_1 is nontrivial and q_2 trivial, the composite number $q_1 \times q_2 \pmod n$ is nontrivial; it reveals the same decomposition as q_1.

- when q_1 and q_2 are nontrivial and $\Delta_1=\pm\Delta_2$, the composite number $q_1 \times q_2 \pmod n$ is trivial; it reveals no decomposition.

- when q_1 and q_2 are nontrivial and $\Delta_1\neq\pm\Delta_2$, the composite number $q_1 \times q_2 \pmod n$ is nontrivial; it reveals a third decomposition.

Three numbers $\{q_1,q_2,q_3\}$ give four composite numbers $\{q_1 \times q_2,\ q_1 \times q_3,\ q_2 \times q_3,\ q_1 \times q_2 \times q_3 \pmod n\}$, i.e. a total of seven numbers; m numbers thus give 2^m-m-1 composite numbers, i.e. a total of 2^m-1 numbers.

Let us consider a set of GQ2 keys in general use comprising i base numbers and g_1 to g_i and i private

numbers Q_1 to Q_i giving i numbers q_1 to q_i and therefore i numbers Δ_1 to Δ_i which are roots of the unit. Let us seek to take into account another base number g_{i+1} by a private number Q_{i+1} giving a number q_{i+1} and therefore a root Δ_{i+1}.

- The total of $2^{i+1}-1$ numbers comprises as many nontrivial numbers in each of the two following cases.

  - The root Δ_{i+1} is trivial and at least one root Δ_1 to Δ_i is nontrivial.

  - The root Δ_{i+1} is nontrivial and figures among the $2xi$ roots $\pm\Delta_1$ to $\pm\Delta_i$.

- Where the root Δ_{i+1} is nontrivial and does not figure among the $2xi$ roots $\pm\Delta_1$ to $\pm\Delta_i$, each composite number where q_{i+1} figures is nontrivial.

Consequently when among m numbers q_1 to q_m, at least one is nontrivial, more than half the total of the 2^m-1 numbers are nontrivial.

By definition, we say that $l < f$ nontrivial numbers $\{q_1, q_2, \ldots q_i\}$ are <u>independent</u> relative to the modulus n when each of the 2^l-l-1 corresponding composite numbers is nontrivial, in other words that, in total, the 2^l-1 numbers are all nontrivial. Each of these 2^l-1 numbers then reveals a different decomposition of the modulus n.

When the f prime factors are distinct, there are $2^{f-1}-1$ decompositions of the modulus n. Then, if $f-1$ numbers q are independent, there is a one-to-one correspondence between the $2^{f-1}-1$ decompositions and a total of $2^{f-1}-1$ numbers including the $f-1$ independent numbers and the $2^{f-1}-f$ corresponding composite numbers.

Chinese remainders - Let two numbers a and b be prime between themselves such that $0<a<b$, and two numbers X_a from 0 to $a-1$ and X_b from 0 to $b-1$; it is a matter of determining the unique number X from 0 to $axb-1$ such that $X_a \equiv X (\mathrm{mod} a)$ and $X_b \equiv X (\mathrm{mod} b)$. The number $\alpha \equiv \{b (\mathrm{mod} a)\}^{-1} (\mathrm{mod}\ a)$ is the parameter of the Chinese

remainders. Here is the elementary operation of Chinese remainders.

$x \equiv X_b \ (\mathrm{mod}a)$

$y \equiv X_a - x$; if y is negative, replace y by $y+a$

$z \equiv \alpha x y \ (\mathrm{mod}a)$

$X = z x b + X_b$

To sum up, we write: X = Chinese Remainders (X_a, X_b).

When f prime factors are put into ascending order, from the smallest p_1 to the largest pf, the parameters of the Chinese remainders may be the following (there is one less than prime factors, i.e. $f-1$).

The first parameter is $\alpha \equiv (p_2 (\mathrm{mod}p_1))^{-1} (\mathrm{mod}p_1)$.

The second parameter is $\beta \equiv (p_1 x p_2 (\mathrm{mod}p_3))^{-1} (\mathrm{mod}p_3)$

The i-th parameter is $\lambda \equiv (p_1 x \ldots p_{i-1} (\mathrm{mod}p_1)^{-1} (\mathrm{mod}p_1)$.

And so on.

In $f-1$ elementary operations, a number X is established from 0 to $n-1$ from any set of f components from X_1 to Xf with Xf from 0 to $pf-1$;

- a first result (mod $p_1 x p_2$) with the first parameter,

- then, a second result (mod $p_1 x p_2 x p_3$) with the second parameter,

- up to the final result (mod n= $p_1 x p_2 x \ldots pf$) with the last parameter.

To sum up, given the prime factors p_1 to pf, each element of the ring of the integers modulo n has two equivalent representations:

- f numbers X_1 to Xf, one component per prime factor : $Xf \equiv X(\mathrm{mod}pf)$,

a number X from 0 to $n-1$, X = Chinese remainders (X_1, X_2, to Xf).

Rank of numbers in CG(p) - Let there be an uneven prime number p and a number a smaller than p, i.e. $0<a<p$. By definition, the rank of a relative to p is the

period of the stream $\{X\}$ defined by $\{x_1 = a$; then, for $i \geq 1$, $x_{i+1} \equiv a x x_1 \equiv (\mathrm{mod} p)\}$. By means of the Fermat theorem, we obtain: $x_{1+p} \equiv a^p x x_i \equiv a x x_i \equiv x_{i+1} (\mathrm{mod} p)$. Consequently, the rank of a number a relative to a prime number p is p-1 or a divisor of p-1.

For example, when $(p-1)/2$ is an uneven prime number p', the Galois field CG(p) comprises a number of rank 1: this is 1, a number of rank 2: this is -1, p'-1 numbers of rank p' and p'-1 numbers of rank $2Xp'=p-1$. In CG(p), any number of rank p-1 is a "generator". The denomination is due to the fact that the successive powers of a generator in CG(p) i.e. the terms of the stream $\{X\}$ for the indices from 1 to p-1, form a permutation of all the non nil elements of CG(p).

Let there be a generator y of CG(p). Let us evaluate the rank of the number y (mod$p$) as a function of i and of p-1. When i is prime with p-1, it is p-1. When i divides p-1, it is $(p-1)/i$. In all cases, it is $(p-1)/\mathrm{pgcd}(p-1,i)$.

By definition, the Euler function $\varphi(n)$ is the number of numbers smaller than n and prime with n. In CG(p), there are $\varphi(p-1)$ generators.

By way of illustration, the rank gives a good understanding of the bases of the RSA. The modulus n is the product of f prime factors p_1 to pf with $f \geq 2$. For each prime factor p_j from p_1 to pf the public exponent e must be prime with p_j-1. Then, the key $\langle e, p_j \rangle$ respects the rank of the elements of CG(pf): it permutates the elements of CG(p_j); there exists a number d_j, generally the smallest possible, such that p_j-1 divides eXd_j-1. The key $\langle d_j, p_j \rangle$ inverts the permutation of the elements of CG(p_j). These f permutations, one in each field CG(p_1) to CG(pf) are expressed in the ring of the integers modulo n by the RSA permutation summarised by the public key $\langle e, n \rangle$. There exists a number d, generally the smallest possible, such that ppcm(p_1-1,p_2-1, … pf-1) divides dXe-

1. For each prime factor p_j from p_1 to pf we have $d_j \equiv d \pmod{pf-1}$. The RSA permutation summarised by the public key $\langle e,n \rangle$ is inverted by the private key $\langle d,n \rangle$.

Squares in CG(*p*) - Let us define a number t such that $p-1$ is divisible by 2^t, but not by 2^{t+1}. Each large prime number figures in one category and one alone: $t=1$, $t=2$, $t=3$, $t=4$, and so on. If a sufficiently large number of successive prime numbers is considered, about one in two figures in the first category where p is congruent with 3 (mod 4), one in four in the second where p is congruent with 5 (mod 8), one in eight in the third where p is congruent with 9 (mod 16), one in the 16 in the fourth where p is congruent with 17 (mod 32), and so on; on average, one in 2^t figures in the t-th category where p is congruent with $2^t+1 \pmod{2^{t+1}}$.

Because the numbers x and $p-x$ have the same square in CG(p), the key $\langle 2,p \rangle$ does not permutate CG(p). The "raise to square" function in CG(p) may be represented by an oriented graph where each non nil element of the field has its place. Let us analyse the structure of the graph in branches and in cycles according to the parity of the rank of each element.

- The nil element is fixed. It is 0. The rank is not defined for the nil element to which no other element is connected; the nil element is isolated.

- The unit element is fixed. It is 1, the only element of rank one. All the roots of the unit in CG(p) are in the branch connecting to 1. Let y be a non-quadratic residue of CG(p), no matter which; the key $\langle (p-1)/2^t, p \rangle$ converts y into a 2^{t-1}-th primitive root of -1 denoted by b; in fact, we have $y^{(p-1)/2} \equiv -1 \pmod{p}$. Consequently, in CG($p$), the powers of b for the exponents from 1 to 2^{t-1} are the 2^{t-1} roots of the unit other than 1: they compose the branch connecting to 1.

- The square of any element of even rank is another element whose rank is divided by two. Consequently, each element of even rank is placed in a branch; each branch comprises a rank number divisible by two but not by four, then, if $t \geq 2$, two numbers of rank divisible by four but not by eight, then, if $t \geq 3$, four numbers of rank divisible by eight but not by sixteen, then, if $t \geq 4$, eight numbers of rank divisible by sixteen but not by 32, and so on. All the branches are similar to the branch connected to 1; the 2^{t-1} leaves of each branch are non-quadratic residues; each branch comprises 2^t-1 elements and is connected to an element of uneven rank; there are $(p-1)/2^t$ branches which all have the same length t.

- The square of any element of uneven rank other than the unit element is another element having the same rank. The key $\langle 2,p \rangle$ permutates all the $(p-1)/2^t$ elements of uneven rank. The permutation decomposes into permutation cycles. The number of cycles depends on the factorization of $(p-1)/2^t$. For each divisor p' of $(p-1)/2^t$, there is a cycle comprising the $\varphi(p')$ elements of rank p'. It should be remembered that by definition, the Euler function $\varphi(p')$ is the number of numbers smaller than p' and prime with p'. For example when $p'=(p-1)/2^t$ is prime, the $p'-1$ numbers of rank p' form a large permutation cycle.

Figures 1A to 1D each show a graph fragment for p congruent respectively with 3 (mod 4), 5 (mod 8), 9 (mod 16) and 17 (mod 32).

- The leaves on the branches are shown by white rounds; these are non-quadratic residues.
- The nodes in the branches are shown by grey rounds; these are quadratic elements of even rank.
- The nodes in the cycles are shown by black rounds; these are quadratic elements of uneven rank.

Square roots in CG(*p*)- Knowing that *a* is a quadratic residue of CG(*p*), let us see how to compute a solution to the equation $x^2 \equiv a \pmod{p}$, i.e. "take a square root" in CG(*p*). There are of course several ways of obtaining the same result: reference could be made to pages 31 to 36 of the book by Henri Cohen, *a Course in Computational Algebraic Number Theory*, published in 1993 by Springer in Berlin as volume 138 of the series *Graduate Texts in Mathematics* (GTM 138).

The number $s = (p-1+2^t)/2^{t-1}$ gives a key $\langle s,p \rangle$ which is worth:

$\langle (p+1)/4,p \rangle$ when *p* is congruent with 3 (mod 4),
$\langle (p+3)/8,p \rangle$ when *p* is congruent with 5 (mod 8),
$\langle (p+7)/16,p \rangle$ when *p* is congruent with 9 (mod 16),
$\langle (p+15)/32,p \rangle$ when *p* is congruent with 17 (mod 32),
and so on.

The key $\langle s,p \rangle$ converts any element in a cycle into the previous element in the cycle. When *a* is of uneven rank, it is the solution of uneven rank; we name it *w*. Indeed, in CG(*p*), w^2/a is worth *a* raised to the power $(2X(p-1+2^t/2^{t-1})-1=(p-1)/2^t$. The other solution is of even rank; it is *p*-*w*.

In a general way, the key $\langle s,p \rangle$ converts any quadratic residue *a* into a first solution approximation which we name *r*. Since *a* is a quadratic residue, the key $\langle 2^{t-1},p \rangle$ certainly converts r^2/a into 1. To get close to a square root of *a*, let us raise r^2/a to the power 2^{t-2} (mod *p*) to obtain +1 or -1. The new approximation remains *r* if the result is +1 or else becomes *b*x*r* (mod *p*) if the result is -1, knowing that *b* denotes any 2^t-th primitive root of 1 in the field CG(*p*). Consequently, the key $\langle 2^{t-2},p \rangle$ converts the new approximation into 1. It is also possible to get close by using the key $\langle 2^{t-3},p \rangle$ and by multiplying by b^2 (mod *p*) if necessary, and so on.

The following algorithm solves the equation. It uses the numbers *a*, *b*, *p*, *r* and *t* defined above and two

variables: c represents successive corrections and w the successive approximations. At the beginning of the algorithm, $c=b$ and $w=r$. At the end of the computation, the two solutions are w and $p-w$.

For i going from $t-2$ to 1, repeat the following sequence:

- Apply the key $\langle 2^t, p\rangle$ to the number $w^2/a \pmod p$ to obtain +1 or -1.
- When -1 is obtained, replace w by $w \times c \pmod p$.

Replace c by $c^2 \pmod p$.

Applicability of principles - By definition we say that a parameter k, a base number g and a prime factor p are compatible when the equation $x^v \equiv g^2 \pmod p$ where the exponent v is worth 2^k has solutions in x in the field CG(p). The numbers k and g are small and larger than 1. The number p is a large prime number.

- When $t=1$, i.e. $p \equiv 3 \pmod 4$, the equation has two solutions.

- When $t=2$, i.e. $p \equiv 5 \pmod 8$, according to the Legendre symbol of g relative to p, the equation has four solutions if $(g|p)=+1$; it has no solution if $(g|p)=-1$.

- When $t>2$, i.e. $p \equiv 1 \pmod 8$, let u be the number such that 2^k divides the rank of the public number $G = g^2$ relative to p, but that 2^{u+1} does not divide it; consequently, u is equal to one of the numbers from 0 to $t-1$. The equation has no solution if $u>0$ and $k+u>t$; it has 2^k solutions if $k+u \leq t$; it has 2^t solutions if $u=0$ and $k>t$.

There are therefore two types of compatibility according to whether G is in a cycle or else in an appropriate position in a branch.

- When G is in a cycle, i.e. $u=0$ whatever the value of k, there is a solution of uneven rank in the cycle and solutions of even rank disseminated in $\alpha=\min(k,t)$ consecutive branches connected to the cycle, i.e.

2^{α} solutions in all. Figure 2A shows this case with $k \geq t=3$, i.e. a prime factor congruent with 9(mod 16), which imposes $u=0$.

- When G is in an appropriate position in a branch, i.e. $u>0$ and $u+k \leq t$, there are 2^k solutions, all of even rank and in the branch. Figure 2B shows this case.

Given a parameter k, there are therefore two types of prime factors according to whether the value of t is lower than k or else higher than or equal to k.

- For any prime factor p_j such that $t<k$, each G_i must be in a cycle and there is no solution in the branch connected to G_i. Let us define a number Δ_{ij} which is worth +1 or -1 depending on whether g_i or $-g_i$ is in the cycle. There is no choice for any of the m numbers $\Delta_{1,j}$ to $\Delta_{m,j}$. Figure 3A shows a case $t<k$, G_i is in a cycle with a prime factor p_j congruent with 9 (mod 16), i.e., $u=0$, $t=3$ with $k>3$.

- For any prime factor p_j such that $t \geq k$, each G_1 must be such that $u+k \leq t$, in other words, or else in a cycle with $u=0$ or else in an appropriate position in a branch with $1 \leq u \leq t-k$. Let us define a number Δ_{ij} which is worth +1 or -1 depending on whether Q_{1j} is in the part of the graph connected to g_i or $-g_i$. There is the choice for each of the m numbers $\Delta_{1,j}$ to $\Delta_{m,j}$; each number Δ_{1j} may be individually swung from one value to the other. Figure 3B shows a case $t \geq k$: G_i is in a branch with a prime factor p, congruent with 17 (mod 32), i.e., $u=1$, $t=4$ with $k=3$.

Each set of f components $\{\Delta_{i,1}$ to $\Delta_{i,f}\}$ is a square root of the unit in $CG(pf)$. This root is trivial or nontrivial according to whether the f components are equal or not; we then say that the set of f components is constant or variable, which expresses the fact that the number q_i is trivial or nontrivial. Consequently,

when a number q_i is nontrivial, the set of f components $\{\Delta_{i,1}$ to $\Delta_{i,f}\}$ summarises a decomposition of the module. It is then possible to test the principles before computing the private components $Q_{i,j}$.

- When a public number G_i is in a cycle for a prime factor p_j, the number $\Delta_{i,j}$ is worth +1 or -1 according to whether g_i or $-g_i$ is in the cycle. When $p_j \equiv 3 \pmod 4$, it is the Legendre symbol: $\Delta_{i,j} = (g_i | p_j)$.

- When a public number G_i is in an appropriate position in a branch for a prime factor p_j, the value to be given to $\Delta_{i,j}$ may be determined before computing the private component $Q_{i,j}$.

Production of sets of keys - Given a parameter k, there are two strategies.

- Either the generator requires f prime factors in order to determine m base numbers. The first prime numbers: 2,3,5,7, etc. are examined to evaluate their compatibility with each of the f large prime factors p_1 to pf. Although g=2 is not compatible with $p \equiv 5 \pmod 8$, 2 can come into the composition of a base number. Indeed, when two numbers are in a similar position in a branch, their product is closer to the cycle, just as a square comes closer to the cycle. A base number can be obtained in this way by composing numbers which are individually not appropriate.

- Or the generator requires m base numbers and modulus characteristics such as a bit size (for example, 512, 768, 1024, 1536, 2048) and a number of high order bits following 1 (for example, 1,8, 1 6, 24, 32) in order to determine $f \geq 2$ prime factors. Denoted by g_1, g_2 ... g_m, the base numbers generally figure among the first prime numbers: 2,3,5,7,11, etc. or else they are combinations of the first prime numbers. Unless otherwise indicated, these are the m first prime numbers: g_1 =2, g_2=3, g_3=5, g_4=7, etc. It should be noted that $p \equiv 5 \pmod 8$ is not compatible with g=2. The modulus

n will be the product of f prime factors of neighbouring sizes, namely the size allocated to the modulus divided by f.

First principle - The parameter k, each prime factor p going from p_1 to pf and each base number g going from g_1 to g_m must be compatible. Let us define a number h such that 2^h divides the rank of g relative to p, whereas 2^{h+1} does not divide it. To compute the number h, the following procedure uses the Legendre symbol $(g|p)$ and a number b, 2^t-th primitive root of the unit in $CG(p)$.

- If $(g|p)=+1$ with $t=1$, return "$h=0$".
- If $(g|p)=+1$ with $t>1$, apply the key $\langle p-1+2^t)/2^{t+1},p\rangle$ to G to obtain a result called w.
- If $w=+g$, return "$h=0$".
- If $w=p-g$, return "$h=1$".
- If not, put c to b and for i going from $t-1$ to 2,
- apply the key $\langle 2^i,p\rangle$ to w/g (mod p) to obtain ±1,
- if -1, put h to i and replace w by wXc (mod p),
- replace c by c^2 (mod p).
- Return "value of h from 2 to $t-1$".
- If $(g|p)=-1$, return "h=t".

Let us remember that k, g and p are incompatible when $u>0$ with $k+u>t$; they are compatible when h=0 or 1, whatever the value of k, and also when $h>1$ with $k+h\leq t+1$.

Second principle - the three following procedures correspond to different implementations of the second principle. In some implementations, the second principle can be reinforced to the extent of demanding that each number q_1 to q_m is nontrivial. The role of the base numbers is then balanced; the fact of balancing or not balancing the second principle has an effect on some aspects of demonstration of the security of the pattern. Finally when there are $f>2$ distinct prime factors, among the m numbers $\{q_1$ to $q_m\}$, it is possible to demand that

there is at least one subunit of f-1 independent numbers.

The three procedures use mx$f$ numbers $\delta_{i,j}$, defined as follows.

- When p_j is such that $t<k$, for i going from 1 to m, $\delta_{i,j}= \Delta_{i,j}$, i.e. +1 if $h_{i,j} = 0$ and −1 if $h_{i,j}=1$.
- When p_j is such that $t\geq k$, for i going from 1 to m, $\delta_{i,j}= 0$, which shows that $\Delta_{1,j}$ to $\Delta_{m,j}$ can be chosen as a function of the second principle.

A first procedure verifies that at least one set $\{\delta_{i,1}$ to $\delta_{i,f}\}$ is variable or nil, in other words that at least one number q_1 to q_m is nontrivial or may be chosen nontrivial.

- For i going from 1 to m and j going from 1 to f,
  - If $\delta_{i,j} = 0$ or $\neq \delta_{i,1}$, return "success".
- Return "failure"

A second procedure verifies that each set $\{\delta_{i,1}$ to $\delta_{i,f}\}$ is variable or nil, in other words that at least one number q_1 to q_m is nontrivial or may be chosen nontrivial.

- For i going from 1 to m
  - for j going from 1 to f,
    - if $\delta_{i,j}=0$ or $\neq\delta_{i,1}$, go to the next value of i.
  - Return "failure"
- Return "success".

A third procedure verifies that for each pair of prime factors p_{j1} and p_{j2} with $1\leq j_1<j_2\leq f$, there is at least one set $\{\delta_{i,1}$ to $\delta_{i,f}\}$ where $\delta_{i,j1}$ is nil or different from $\delta_{i,j2}$. It fails manifestly when m is smaller than f-1. When it succeeds, among the m numbers q_1 to q_m, there is at least one set of f-1 independent numbers relative to the f prime factors.

- For j_1 going from 1 to f-1 and for j_2 going from j_1+1 to f,
  - for i going from 1 to m,

- if $\delta_{i,\ j1}=0$ or $\neq\delta_{i,j2}$, go to the next values of j_1 and j_2.
- Return "failure"

- Return "success".

When a procedure fails, the generator of sets of GQ2 keys follows a strategy among the two possible strategies:

- change one of the m base numbers while keeping the f prime factors,
- change one of the f prime factors while keeping the m base numbers.

Third principle - the following procedure determines whether the set of generalized GQ2 keys in the course of production or already produced is:

- a set of GQ2 elementary keys, in other words that the $2Xm$ numbers $\pm g_1$ to $\pm g_m$ are all non-quadratic residues,
- or else, a set of GQ2 complementary keys, in other words that among the $2xm$ numbers $\pm g_1$ to $\pm g_m$, there is at least one quadratic residue.

The procedure uses the two Legendre symbols $(g_i|p_j)$ and $(-g_i|p_j)$ for i going from 1 to m and for j going from 1 to f.

- For i going from 1 to m
  - for j going from 1 to f,
    - if $(g_i|p_j) = -1$, go to the next value of i.
  - Return "set of GQ2 complementary keys".
  - for j going from 1 to f,
    - if $(-g_i|p_j) = -1$, go to the next value of i.
  - Return "set of GQ2 complementary keys".
- Return "set of GQ2 elementary keys".

Private components - for an equation of the direct type: $x^v \equiv g_1^{\ 2} \pmod{p_j}$, the following computations

establish all the possible values of the private component $Q_{i,j}$. The two simplest and most common cases, i.e. t=1 and t=2, are followed by the most complex case, i.e. t>2.

For t=1, i.e. $p_j \equiv 3 \pmod 4$, the key $\langle (p_j+1)/4, p \rangle$ gives the square quadratic root of any quadratic residue in $CG(p_j)$. A number $s_j \equiv ((p_j+1)/4)^k \pmod{(p_j-1)/2}$ is deduced, which gives a key $\langle s_j, p_j \rangle$ converting G_1 into $w \equiv G_1^{sj} \pmod{p_j}$. $Q_{i,j}$ is equal to w or else to p_j-w.

For t=2, i.e. $p_j \equiv 5 \pmod 8$, the key $\langle (p_j+3)/8, p_j \rangle$ gives the square root of uneven rank of any element of uneven rank in $CG(p_j)$. A number $s_j \equiv ((p_j+3)/8)^k \pmod{(p_j-1)/4}$ is deduced, which gives a key $\langle s_j, p_j \rangle$ converting G_i into $w \equiv G_i^{sj} \pmod{(p_j)}$. It should be observed that $z \equiv 2^{(pj-1)/4} \pmod{p_j}$ is a square root of -1 because 2 is a non-quadratic residue in $CG(p_j)$. $Q_{i,j}$ is equal to w or else to p_j-w or else to $w' \equiv wxz \pmod{p_j}$ or else to p_j-w'.

For $p_j \equiv 2^t+1 \pmod{2^{t+1}}$ with t>2, the key $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ gives the square root of uneven rank of any element of uneven rank. The compatibility test between k, g and p has given the value of h, then that of u.

- When G_i is in a cycle (u=0, whatever the value of k), a number $s_j \equiv ((p_j-1+2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t}$ is established. The key $\langle s_j, p_j \rangle$ converts G_i into the solution of uneven rank $G_i^{sj} \pmod{p_j}$. There are solutions of even rank distributed in $\min(k,t)$ consecutive branches tied to the cycle, let us say in α branches. $Q_{i,j}$ is equal to the product of w by any of the 2^{α}-th roots of the unit in $CG(p_j)$.

- When G_i is in an appropriate position in a branch (u>0, $u+k \leq t$), all the solutions are in the same branch as G_i, a branch tied to a cycle by the 2^u-th power of the number G_i. A number $s_j \equiv ((p_j-1+2^t)/2^{t+1})^{k+u} \pmod{(p_j-1)/2^t}$ is established. The key $\langle s_j, p_j \rangle$ converts the 2^u-th power of G_i into a number of uneven rank w. All the

products of w by the 2^{k+u}-th primitive roots of the unit in CG(p_j) include the 2^k values of $Q_{i,j}$.

When p_j is such that $t \geq k$, the number b_j being a 2^t-th primitive root of the unit in CG(p_j), the 2^{t-u}-th power of b_j in CG(p_j) exists; it is a 2^k-th primitive root of the unit. Multiplying $Q_{i,j}$ by a 2^k-th primitive root of the unit allows the value of the number $\Delta_{i,j}$ to be swung.

For an equation of the inverse type: $1 \equiv x^v x g_i^2 \pmod{p_j}$, it is sufficient to replace the number s_j by $((p_j-1)/2^t) - s_j$ in the key $\langle s_j, p_j \rangle$, which amounts to inverting the value of $Q_{i,j}$ in CG(p_j).

Example of a set of keys with two prime factors congruent with 5 (mod8)

p_1=E6C83BF428689AF8C35E07EDD06F9B39A659829A58B79CD894C435C95F32BF25

p_2=11BF8A68A0817BFCC00F15731C8B70CEF9204A34133A0DEF862829B2EEA74873D

n=p_1Xp_2=FFFF8263434F173D0F2E76B32D904F56F4A5A6A50008C43D32B650E9AB9AAD2EB713CD4F9A97C4DBDA3828A3954F296458D5F42C0126F5BD6B05478BE0A80ED1

Here are the Legend symbols of the very first prime numbers.

$(2|p_1) = -1$; $(3|p_1) = -1$; $(5|p_1) = -1$; $(7|p_1) = -1$;
$(11|p_1) = +1$; $(13|p_1) = -1$; $(17|p_1) = +1$;

In CG(p_1) the rank is uneven for -5, -11 and 17.

$(2|p_2) = -1$; $(3|p_2) = +1$; $(5|p_2) = +1$; $(7|p_2) = +1$;
$(11|p_2) = +1$; $(13|p_2) = -1$; $(17|p_2) = -1$;

In CG(p_2) the rank is uneven for 3, -5, 7 and 11.

The Carmichael function is $\lambda(n)$=ppcm($(p_1-1)/4$, $(p_2-1)/4$).

$\lambda(n)$=33331A13DA4304A5CFD617BD6F83431164212154333 4F40C3D5 7A9C8558555D5BDAA2EF6AED17B9E3794F51A65A1B37239B18FA9B0F 618627D8C7E1D8499C1B

With k=9, the number $\sigma \equiv \lambda(n) - ((1+\lambda(n))/2)^9 \pmod{\lambda(n)}$ as private exponent, so as to use generic equations of the inverse type.

σ=01E66577BC997CAC273671E187A35EFD25373ABC9FE6770E7446C0 CCEF2C72AF6E89D0BE277CC6165F1007187AC58028BD2416D4CC1121 E7A7A8B6AE186BB4B0

The numbers 2,3,7,13 and 17 are not suitable as a base number.

The key $\langle \sigma, n \rangle$ converts g_1=5 into a private number Q_1 which shows no decomposition. Indeed, in both fields, -5 is on a cycle.

Q_1=818C23AF3DE333FAECE88A71C4591A70553F91D6C0DD5538EC0F2A AF909B5BDAD491FD8BF13F18E3DA3774CCE19D0097BC4BD47C5D6E0E 7EBF6D89FE3DC5176C

The key $\langle \sigma, n \rangle$ converts g_2=11 into a private number Q_2 which shows decomposition. Indeed, 11 is not in the same position in the two fields.

Q_2=25F9AFDF177993BE8652CE6E2C728AF31B6D66154D3935AC535196 B07C19080DC962E4E86ACF40D01FDC454F2565454F290050DA052089 EEC96A1B7DEB92CCA7

The key $\langle \sigma, n \rangle$ converts g_3=21=3x7 into a private number Q_3 which shows decomposition.

Q_3=78A8A2F30FEB4A5233BC05541AF7B684C2406415EA1DD67D18A045 9A1254121E95D5CAD8A1FE3ECFE0685C96CC7EE86167D99532B3A96B 6BF9D93CAF8D4F6AF0

The key $\langle \sigma, n \rangle$ converts g_4=26=2x13 into a private number Q_4 which shows decomposition.

Q_4=6F1748A6280A200C38824CA34C939F97DD2941DAD300030E481B738C62BF8C673731514D1978AF5655FE493D659514A6CE897AB76C01E50B5488C5DAD12332E5

The private key may still be represented by the two prime factors, the parameter of the Chinese remainders and eight private components.

$\alpha \equiv (p_2 \pmod{p_1})^{-1} \pmod{p_1}$ =
ADE4E77B703F5FDEAC5B9AAE825D649E06692D15FBF0DF737B115DC4D012FD1D

$Q_{1,1} \equiv Q_1 \pmod{p_1}$ =
7751A9EE18A8F5CE44AD73D613A4F465E06C6F9AF4D229949C74DD6C18D76FAF

$Q_{1,2} \equiv Q_1 \pmod{p_2}$ =A9EB5FA1B2A981AA64CF88C382923DB64376F5FD48152C08EEB6114F31B7665F

$Q_{2,1} \equiv Q_2 \pmod{p_1}$ =D5A7D33C5FB75A033F2F0E8B20274B957FA34004ABB2C2AC1A3F5320C5A9049

$Q_{2,2} \equiv Q_2 \pmod{p_2}$ =76C9F5EFD066C73A2B5CE9758DB512DFC011F5B5AF7DA8D39A961CC876F2DD8F

$Q_{3,1} \equiv Q_3 \pmod{p_1}$ =2FEC0DC2DCA5BA7290B27BC8CC85C938A514B8F5CFD55820A174FB5E6DF7B883

$Q_{3,2} \equiv Q_3 \pmod{p_2}$ =010D488E6B0A38A1CC406CEE0D55DE59013389D8549DE493413F34604A160C1369

$Q_{4,1} \equiv Q_4 \pmod{p_1}$ =A2B32026B6F82B6959566FADD9517DB8ED8524652145EE159DF3DC0C61FE3617

$Q_{4,2} \equiv Q_4 \pmod{p_2}$ =011A3BB9B607F0BD71BBE25F52B305C224899E5F1F8CDC2FE0D8F9FF62B3C9860F

Polymorphism of the GQ2 private key - The different possible representations of the GQ2 private key prove to be equivalent: they all come back to the knowledge of

the factorization of the modulus n which is the true GQ2 private key. The representation of the GQ2 private key has an effect on the operation of the computations within the proving entity, not within the controlling entity. Here are the three main possible representations of the GQ2 private key. 1) The conventional representation of GQ private keys consists in storing m private numbers Q_i and the public verification key $\langle v,n \rangle$; for GQ2 patterns, this representation is in competition with the two which follow. 2) the optimum representation in terms of work loads consists in storing the parameter k, the f prime factors p_j, mx$f$ private components $Q_{i,j}$ and f-1 parameters of the Chinese remainders. 3) the optimum representation in terms of private key size consists in storing the parameter k, the m base numbers g_i, the f prime factors p_j, then, in starting each usage by establishing either m private numbers Q_i and the modulus n to come back to the first representation, or else mx$f$ private components $Q_{i,j}$ and f-1 parameters of the Chinese remainders to come back to the second.

Because the security of the dynamic authentication or digital signature mechanism is equivalent to knowledge of a decomposition of the modulus, GQ2 patterns do not allow a simple distinction to be made between two entities using the same modulus. Generally, each proving entity has its own GQ2 modulus. However, it is possible to specify GQ2 moduli with four prime factors two of which are known by one entity and the two others by another.

Dynamic authentication - The dynamic authentication mechanism, which is intended to prove to an entity called a **controller**, the authenticity of another entity called a **demonstrator** and the authenticity of any associated message M, so that the controller can be sure that it is the actual demonstrator and possibly that he and the demonstrator are in fact speaking about the same

message *M*. The associated message *M* is optional, which means that it may be empty.

The dynamic authentication mechanism is a sequence of four acts: an act of commitment, an act of challenge, an act of response and an act of checking. The demonstrator performs the acts of commitment and response. The controller performs the acts of challenge and control.

Within the demonstrator, a witness may be isolated, in such a way as to isolate the most sensitive parameters and functions of the demonstrator, in other words, the production of commitments and responses. The witness has at its disposal the parameter *k* and the GQ2 private key, in other words, the factorization of the modulus *n* according to one of the three representations mentioned above: • the *f* prime factors and the *m* base numbers, • the m*x*f private components, the *f* prime factors and *f*-1 parameters of the Chinese remainders, • the *m* private numbers and the modulus n.

The witness may correspond to a particular embodiment, for example, • a chip card linked to a PC together forming the demonstrator, or again, • specially protected programs within a PC, or again, • specially protected programs within a chip card. The witness so isolated is similar to the witness defined hereinafter within the signatory. With each operation of the mechanism, the witness produces one or more commitments *R*, then, as many responses *D* to as many challenges *d*. Each set {*R,d,D*} constitutes a **GQ2 triplet.**

The demonstrator not only includes the witness, but also has at its disposal, where necessary, a hashing function and a message M.

The controller has at its disposal the modulus n, for example, from a directory of public keys or again from a register of public keys; where necessary, it also has at its disposal the same hashing function and a

message M'. The GQ2 public parameters, namely the numbers k, m and g_1 to g_m may be given to the controller by the demonstrator. The controller is able to restore a commitment R' from any challenge d and from any response D. The parameters k and m inform the controller. Unless otherwise indicated, the m base numbers from g_1 to g_m are the m first prime numbers. Each challenge d must comprise m elementary challenges denoted from d_1 to d_m: one per base number. Each elementary challenge from d_1 to d_m is a number from 0 to $2^{\lambda-1}-1$ (the numbers from $v/2$ to $v-1$ are not used). Typically, each challenge is encoded by m times $k-1$ bits (and not by m times k bits). The example, with $k=5$ and $m=4$ base numbers 5, 11, 21, and 26, each challenge comprises 16 bits transmitted on four quartets. When the $(k-1)xm$ possible challenges are also probable, the number $(k-1)xm$ determines the security brought by each GQ2 triplet: an impostor who, by definition, does not know the factorization of the modulus n has exactly 1 chance of success in $2^{(k-1)xm}$. When $(k-1)xm$ is worth from 15 to 20, one triplet is enough to reasonably ensure dynamic authentication. To reach any level of security, triplets may be produced in parallel: they may also be produced in sequence, in other words, repeat the operation of the mechanism.

1) **The act of commitment** includes the following operations.

When the witness does not use Chinese remainders, it has at its disposal the parameter k, the m private numbers from Q_1 to Q_m and the modulus n; it draws at random and in private one or more random numbers r $(0<r<n)$; then, by k successive raisings to the square (mod n), it converts each random number r into a commitment R.

$$R \equiv r^v \pmod{n}$$

Here is an example with the previous set of keys without the Chinese remainders.

r=5E94B894AC24AF843131F437C1B1797EF562CFA53AB8AD426C1AC0
16F1C89CFDA13120719477C3E2FB4B4566088E10EF9C010E8F09C60D
981512198126091996

R=6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E3300EB
F234FA0BC20A95152A8FB73DE81FAEE5BF4FD3EB7F5EE3E36D7068D0
83EF7C93F6FDDF673A

When the witness uses Chinese remainders, it has at its disposal the parameter k, the f prime factors from p_1 to pf, f-1 parameters of the Chinese remainders and the mx$f$ private components $Q_{i,j}$; it draws at random and in private one or more collections of f random numbers: each collection comprises one random number r_i per prime factor p_i ($0<r_i<p_i$); then, by k successive raisings to the square (mod p_i), it converts each random number r_i into a commitment component R_i.

$$R_i \equiv r_i^{v} \pmod{p_i}$$

For each collection of f commitment components, the witness establishes a commitment according to the technique of Chinese remainders. There are as many commitments as collections of random numbers.

$$R = \text{Chinese Remainders } (R_1,\ R_2,\ \text{to } Rf)$$

Here is an example with the previous set of keys and with Chinese remainders.

r_1=5C6D37F0E97083C8D120719475E080BBBF9F7392F11F3E244FDF02
04E84D8CAE

R_1=3DDF516EE3945CB86D20D9C49E0DA4D42281D07A76074DD4FEC5C7
C5E205DF66

r_2=AC8F85034AC78112071947C457225E908E83A2621B0154ED15DBFC B9A4915AC3

R_2=01168CEC0F661EAA15157C2C287C6A5B34EE28F8EB4D8D340858079BCAE4ECB016

R = Chinese Remainders (R_1, R_2)= 0AE51D90CB4FDC3DC757C56E063C9ED86BE153B71FC65F47C123C27F082BC3DD15273D4A923804718573F2F05E991487D17DAE0AAB7DF0D0FFA23E0FE59F95F0

In both cases, the demonstrator transmits to the controller all or part of each commitment R, or else, a hashing code H obtained by hashing each commitment R and a message M.

2) **The act of challenge** consists in drawing at random one or more challenges d each composed of m elementary challenges d_1, d_2 to d_m; each elementary challenge d_1 is one of the numbers from 0 to $v/2-1$.

$$d = d_1, d_2 \ldots d_m$$

Here is a challenge for the two examples, in other words with k=5 and m=4.

d_1=1011=11='B'; d_2 = 0011=3; d_3 =0110=6; d_4 =1001=9,

$d = d_1 \,||d_2||d_3||\, d_4$= 10110011 01101001=B3 69

The controller transmits each challenge d to the demonstrator.

3) **The act of response** comprises the following operations.

When the witness does not use Chinese remainders, it has at its disposal the parameter k, the m private numbers from Q_1 to Q_m and the modulus n; it computes one or more responses D by using each random number r of the act of commitment and the private numbers in accordance with the elementary challenges.

$$D \equiv r \times Q_1^{d1} \times Q_2^{d2} \times \ldots Q_m^{dm} \pmod{n}$$

Here is the sequence of the example without the Chinese remainders.

D=027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A7870E6C1940F7A6996C2D871EBE611812532AC5875E0E116CC8BA648FD8E86BE0B2ABCC3CCBBBE4

When the witness uses Chinese remainders, it has at its disposal the parameter k, the f prime factors from p_1 to pf, f-1 parameters of the Chinese remainders and the mx$f$ private components $Q_{1,j}$; it computes one or more collections of f response components by using each collection of random numbers of the act of commitment: each collection of response components comprises one component per prime factor.

$$D_i \equiv r_i \times Q_{1,i}^{d1} \times Q_{2,i}^{d2} \times \ldots Q_{m,i}^{dm} \pmod{p_i}$$

For each collection of response components, the witness establishes a response in accordance with the technique of Chinese remainders. There are as many responses as challenges.

$$D = \text{Chinese Remainders } (D_1, D_2, \ldots Df)$$

Here is the sequence of the example with Chinese remainders.

$D_1 = r_1 \times Q_{1,1}^{d1} \times Q_{2,1}^{d2} \times Q_{3,1}^{d3} \times Q_{4,1}^{d4} \pmod{p_i} =$
C71F86F6FD8F955E2EE434BFA7706E38E5E715375BC2CD2029A4BD572A9EDEE6

$D_2 = r_2 \times Q_{1,2}^{d1} \times Q_{2,2}^{d2} \times Q_{3,2}^{d3} \times Q_{4,2}^{d4} \pmod{p_2} =$

0BE022F4A20523F98E9F5DBEC0E10887902F3AA48C864A6C354693AD
0B59D85E
D=90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98C8577
A660B9CFCEAECB93BE1BCC356811BF12DD667E2270134C9073B9418C
A5EBF5191218D3FDB3

In both cases, the demonstrator transmits each response *D* to the controller.

4) **The act of checking** consists in checking that each triplet $\{R, d, D\}$ verifies an equation of the following type <u>for a non nil value</u>,

$$R \times \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{or else} \quad R \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

or else, in re-establishing each commitment: <u>none must be nil.</u>

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{or else} \quad R' \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Possibly, the controller next computes a hashing code *H′* by hashing each re-established commitment *R′* and a message *M′*. The dynamic authentication is successful when the controller thus regains what it received at the end of the act of commitment, in other words, all or part of each commitment *R*, or else, the hashing code *H*.

For example, a sequence of elementary operations converts the response *D* into a commitment *R′*. The sequence includes *k* squares (mod *n*) separated by *k*-1 divisions or multiplications (mod *n*) by base numbers. For the *i*-th division or multiplication, which is carried out between the *i*-th square and the i+1-th square, the *i*-th bit of the elementary challenge d_1 indicates whether it is necessary to use g_1, the *i*-th bit of the elementary challenge d_2 indicates whether it is

necessary to use g_2, up to the i-th bit of the elementary challenge d_m which indicates whether it is necessary to use g_m.

Here is the end of the example without the Chinese remainders.

D=027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A7870E
6C1940F7A6996C2D871EBE611812532AC5875E0E116CC8BA648FD8E8
6BE0B2ABCC3CCBBBE4

Raise to the square modulo n:

88BA681DD641D37D7A7D9818D0DBEA82174073997C6C32F7FCAB3038
0C4C6229B0706D1AF6EBD84617771C31B4243C2F0376CAF5DCEB644F
098FAF3B1EB49B39

Multiply by 5 times 26 = 130, i.e. '82' modulo n:

6ECABA65A91C22431C413E4EC7C7B39FDE14C9782C94FD6FA3CAAD7A
FE192B9440C1113CB8DBC45619595D263C1067D3D0A840FDE008B415
028AB3520A6AD49D

Raise to the square modulo n:

0236D25049A5217B13818B39AFB009E4D7D52B17486EBF844D64CF75
C4F652031041328B29EBF0829D54E3BD17DAD218174A01E6E3AA650C
6FD62CC274426607

Multiply by 21, i.e. '15' modulo n:

2E7F40960A8BBF1899A06BBB6970CFC5B47C88E8F115B5DA594504A9
2834BA405559256A705ABAB6E7F6AE82F4F33BF9E91227F0ACFA4A05
2C91ABF389725E93

Raise to the square modulo n:

B802171179648AD687E672D3A32640E2493BA2E82D5DC87DBA2B2CC0
325E7A71C50E8AE02E299EF868DD3FB916EBCBC0C5569B53D42DAD49
C956D8572E1285B0

Multiply by 5 times 11 times 21 = 1155, i.e. '483' modulo *n*:

3305560276310DEFEC1337EB5BB5810336FDB28E91B350D485B09188
E0C4F1D67E68E9590DB7F9F39C22BDB45330136250112 48A8DC417C6
67B419D27CB11F72

Raise to the square modulo *n*:

8871C494081ABD1AEB8656C38B9BAAB57DBA72A4BD4EF9029ECBFFF5
40E55138C9F22923963151FD0753145DF70CE22E9D019990E41DB610
4005EEB7B1170559

Multiply by 5 times 11 times 26 = 1430, i.e. '596' modulo *n*:

2CF5F76EEBF128A0701B56F837FF68F81A6A5D175D0AD67A14DAEC6F
B68C362B1DC0ADD6CFC004FF5EEACDF794563BB09A17045ECFFF88F5
136C7FBC825BC50C

Raise to the square modulo *n*:

6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E3300EBF2
34FA0BC20A95152A8FB73DE81FAEE5BF4FD3EB7F5EE3E36D7068D083
EF7C93F6FDDF673A

The commitment *R* is found. The authentication is successful.

Here is the end of the example with Chinese remainders.

D=90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98C8577
A660B9CFCEAECB93BE1BCC356811BF12DD667E2270134C9073B9418C
A5EBF5191218D3FDB3

Raise to the square modulo *n*:

770192532E9CED554A8690B88F16D013010C903172B266C1133B136E
BE3EB5F13B170DD41F4ABE14736ADD3A70DFA43121B6FC5560CDD4B4
845395763C792A68

Multiply by 5 times 26 = 130, i.e. '82' modulo *n*:

6EE9BEF9E52713004971ABB9FBC31145318E2A703C8A2FB3E144E778
6397CD8D1910E70FA86262DB771AD1565303AD6E4CC6E90AE3646B46
1D3521420E240FD4

Raise to the square modulo *n*:

D9840D9A8E80002C4D0329FF97D7AD163D8FA98F6AF8FE2B2160B212
6CBBDFC734E39F2C9A39983A426486BC477F20ED2CA59E664C23CA0E
04E84F2F0AD65340

Multiply by 21, i.e. '15' modulo *n*:

D7DD7516383F78944F2C90116E1BEE0CCDC8D7CEC5D7D1795ED33BFE
8623DB3D2E5B6C5F62A56A2DF4845A94F32BF3CAC360C7782B594192
4BB4BE91F86BD85F

Raise to the square modulo *n*:

DD34020DD0804C0757F29A0CBBD7B46A1BAF949214F74FDFE021B626
ADAFBAB5C3F1602095DA39D70270938AE362F2DAE0B914855310C7BC
A328A4B2643DCCDF

Multiply by 5 times 11 times 21 = 1155, i.e. '483' modulo *n*:

038EF55B4C826D189C6A448EFDD9DADBD2B63A7D675A0587C8559618
EA2D83DF552D24EAF6BE983FB4AFB3DE7D4D2545190F1B1F946D327A
4E9CA258C73A98F57

Raise to the square modulo *n*:

D1232F50E30BC6B7365CC2712E5CAE079E47B971DA03185B33E918EE
6E99252DB3573CC87C604B327E5B20C7AB920FDF142A8909DBBA1C04
A6227FF18241C9FE

Multiply by 5 times 11 times 26 = 1430, i.e. '596' modulo *n*:
3CC768F12AEDFCD4662892B9174A21D1F0DD9127A54AB63C984019BE
D9BF88247EF4CCB56D71E0FA30CFB0FF28B7CE45556F744C1FD751BF
BCA040DC9CBAB744

Raise to the square modulo *n*:

0AE51D90CB4FDC3DC757C56E063C9ED86BE153B71FC65F47C123C27F
082BC3DD15273D4A923804718573F2F05E991487D17DAE0AAB7DF0D0
FFA23E0FE59F95F0

The commitment *R* is found. The authentication is successful.

Digital signature

The digital signature mechanism allows an entity called a **signatory** to produce signed messages and an entity called a **controller** to verify signed messages. The message *M* is any binary sequence: it may be empty. The message *M* is signed with an adjoining signature appendix, which includes one or more commitments and/or challenges, as well as the corresponding responses.

The controller has at its disposal the modulus *n*, for example, from a directory of public keys or else from a register of public keys; it also has the same

hashing function. The GQ2 public parameters, namely the numbers k, m and g_1 to g_m may be given to the controller by the demonstrator, for example, by putting them in the signature appendix.

The numbers k, and m inform the controller. On the one hand, each elementary challenge, from d_1 to d_m, is a number from 0 to $2^{k-1}-1$ (the numbers $v/2$ to $v-1$ are not used). On the other hand, each challenge d must comprise m elementary challenges denoted from d_1 to d_m, as many as base numbers. Additionally, unless otherwise indicated, the m base numbers, from g_1 to g_m, are the m first prime numbers. With $(k-1)xm$ being worth from 15 to 20, it is possible to sign with four GQ2 triplets produced in parallel; with $(k-1)xm$ being worth 60 or more, it is possible to sign with a single GQ2 triplet. For example with $k=9$ and $m=8$, a single GQ2 triplet is sufficient; each challenge comprises eight bytes and the base numbers are 2, 3, 5, 7, 11, 13, 17, and 19.

The signature operation is a sequence of three acts: an act of commitment, an act of challenge, and an act of response. Each act produces one or more GQ2 triplets each including: a commitment R ($\neq 0$), a challenge d composed of m elementary challenges denoted by $d_1, d_2, \ldots d_m$ and a response D ($\neq 0$).

The signatory has at its disposal a hashing function, the parameter k and the GQ2 private key, in other words, the factorization of the modulus n according to one of the three representations mentioned above. **Within the signatory, it is possible to isolate a witness who performs the acts of commitment and response**, in such a way as to isolate the most sensitive functions and parameters of the demonstrator. In order to compute commitments and responses, the witness has at its disposal the parameter k and the GQ2 private key, in other words, the factorization of the modulus n according to one of the three representations mentioned

above. The witness so isolated is similar to the witness defined within a demonstrator. It may correspond to one particular embodiment, for example, • a chip card linked to a PC together forming the signatory, or again, • specially protected programs within a PC, or again, • specially protected programs within a chip card.

1) **The act of commitment** includes the following operations.

When the witness has at its disposal m private numbers Q_1 to Q_m and the modulus n, it draws at random and in private one or more random numbers r $(0<r<n)$; then, by k successive raisings to the square (mod n), it converts each random number r into a commitment R.

$$R \equiv r^v \pmod{n}$$

When the witness has at its disposal the f prime factors from p_1 to pf, and the mxf private components Q_{1j}, it draws at random and in private one or more collections of f random numbers: each collection comprises one random number r_i per prime factor p_i $(0<r_i<p_i)$; then, by k successive raisings to the square (mod p_i), it converts each random number r_i into a commitment component R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

For each collection of f commitment components, the witness establishes a commitment according to the technique of Chinese remainders. There are as many commitments as collections of random numbers.

$$R = \text{Chinese Remainders } (R_1,\ R_2,\ \text{to } Rf)$$

2) **The act of challenge** consists in hashing all the commitments R and the message to sign M in order to

obtain a hashing code from which the signatory forms one or more challenges each including m elementary challenges; each elementary challenge is a number from 0 to $v/2-1$; for example, with k=9 and m=8, each challenge comprises eight bytes. There are as many challenges as commitments.

$d = d_1\ d_2\ \ldots\ d_m$, extracted from the Hash result (M, R)

3) **The act of response** comprises the following operations.

When the witness has at its disposal the m private numbers from Q_1 to Q_m and the modulus n, it computes one or more responses D by using each random number r of the act of commitment and the private numbers in accordance with the elementary challenges.

$$X \equiv Q_1^{d1} \times Q_2^{d2} \times \text{to } Q_m^{dm} \pmod{n}$$
$$D \equiv r \times X \pmod{n}$$

When the witness has at its disposal the f prime factors from p_1 to pf, and the m$x$$f$ private components Q_{ij}, it computes one or more collections of f response components by using each collection of random numbers of the act of commitment: each collection of response components comprises one component per prime factor.

$$X_i \equiv Q_{1,i}^{d1} \times Q_{2,i}^{d2} \times \text{to } Q_{m,i}^{dm} \pmod{p_i}$$
$$D_i \equiv r_i \times X_i \pmod{p_i}$$

For each collection of response components, the witness establishes a response in accordance with the technique of Chinese remainders. There are as many responses as challenges.

$$D = \text{Chinese Remainders } (D_1,\ D_2,\ \text{to } Df)$$

The signatory signs the message *M* joining to it a signatory appendix including:

- either, each GQ2 triplet, i.e., each commitment *R*, each challenge *d* and each response *D*,
- or, each commitment *R* and each corresponding response *D*,
- or, each challenge *d* and each corresponding response *D*.

The performance of the verification operation depends on the content of the signature appendix. A distinction can be made between the three cases.

Where the appendix includes one or more triplets, the control operation comprises two independent processes the chronology of which is immaterial. The controller accepts the signed message if and only if the two following conditions are met.

On the one hand, each triplet must be coherent (an appropriate relation of the following type must be verified) and receivable (the comparison must be made on a non nil value).

$$R \times \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \text{ or else } R \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

For example, the response *D* is converted by a sequence of elementary operations: *k* squares (mod *n*) separated by *k*-1 multiplications or divisions (mod *n*) by base numbers. For the *i*-th multiplication or division, which is carried out between the *i*-th square and the i+1-th square, the *i*-th bit of the elementary challenge d_1 indicates whether it is necessary to use g_1, the *i*-th bit of the elementary challenge d_2 indicates whether it is necessary to use g_2, up to the *i*-th bit of the elementary challenge d_m which indicates whether it is necessary to use g_m. In this way each commitment *R* is to be found present in the signature appendix.

On the other hand, the triplet or triplets must be tied to the message *M*. By hashing all the commitments *R* and the message *M*, a hashing code is obtained from which each challenge *d* is to be found.

$d = d_1\ d_2\ \ldots\ d_m$, identical to those extracted from the Hash result (*M*, *R*)

Where the appendix does not include a challenge, the control operation starts with the reconstitution of one or more challenges *d'* by hashing all the commitments R and the message *M*.

$d' = d'_1\ d'_2\ \ldots\ d'_m$, extracted from the Hash result (*M*, *R*)

Next, the controller accepts the signed message if and only if each triplet is coherent (an appropriate relation of the following type is verified) and receivable (the comparison is made on a non nil value).

$$R \times \prod_{i=1}^{m} G_i^{d'_i} \equiv D^{2^k} \pmod{n} \text{ or else } R \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d'_i} \pmod{n}$$

Where the appendix does not include a commitment, the control operation starts with the reconstitution of one or more commitments *R'* according to one of the two following formulas, the one which is appropriate. No re-established commitment must be nil.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \text{ or else } R' \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Next, the controller must hash all the commitments *R'* and the message *M* so as to reconstitute each challenge *d*.

$d = d_1\ d_2\ \ldots\ d_m$, identical to those extracted from the Hash result (*M*, *R'*)

The controller accepts the signed message if and only if each reconstituted challenge is identical to the corresponding challenge featuring in the appendix

CLAIMS

1. A process intended to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity;

said process implementing:

- a public modulus n constituted by the product of f prime factors p_1, p_2 ... p_f (f being greater than or equal to 2) or implementing the f prime factors;
- m different whole base numbers g_1, g_2 ... g_m (m being greater than or equal to 1), g_i being less than the f prime factors p_1, p_2 ... p_f ;
- m pairs of private Q_1, Q_2, ... Q_m and public G_1, G_2, ... G_m values (m being greater than or equal to 1) or parameters derived from them;

said modulus and said private and public values being connected by relations of the type:

$$G_i . Q_i^{\,v} \equiv 1 . \mathrm{mod}\ n \text{ or } G_i \equiv Q_i^{\,v} \bmod n$$

said public value G_i being the square $g_i^{\,2}$ of the base number, v denoting a public exponent of the form:

$$v = 2^k$$

where k is a security parameter greater than 1;

the process according to the invention including the step of producing the f prime factors p_1, p_2 … p_f and/or the m base numbers g_1, g_2 … g_m in such a way that the following conditions are met.

First condition :

According to the first condition, each of the equations:

$$X^v \equiv g_i^2 \bmod n \quad (1)$$

has solutions in x in the ring of the integers modulo n.

Second condition :

where $G_i \equiv Q_i^v \bmod n$, among the m numbers q_i obtained by raising Q_1 to the square modulo n, k-1 times of rank, one of them is different from $\pm g_i$ (in other words is nontrivial).

where $G_1.Q_i^v \equiv 1 \bmod n$, among the m numbers q_i obtained by raising the inverse of Q_1 to the square modulo n, k-1 times of rank, one of them is different from $\pm g_i$ (in other words is nontrivial).

Third condition :

among the 2m equations:

$$X^2 \equiv g_i \bmod n \quad (2)$$
$$X^2 \equiv - g_1 \bmod n \quad (3)$$

at least one of them has solutions in x in the ring of the integers modulo n;

the process according to the invention for producing the f prime factors p_1, p_2 to p_f and/or the m base numbers g_1, g_2 to g_m includes the step of choosing firstly:

- the security parameter k

- the m base numbers g_1, g_2 to g_m and/or the f prime factors p_1, p_2 to p_f.

2. A process according to claim 1 such that the m base numbers g_1, g_2 ... g_m are chosen at least partly among the first whole numbers.

3. A process according to one of the claims 1 or 2 such that the security parameter k is a small whole number, particularly less than 100.

4. A process according to any one of claims 1 to 3 such that the size of the modulus n is more than several hundred bits.

5. A process according to any one of claims 1 to 4 such that the f prime factors p_1, p_2 to p_f, have a size close to the size of the modulus n divided by the number f of factors.

6. A process according to any one of claims 1 to 5 such that to test the first condition, the compatibility of the numbers k, p, g is verified by implementing the algorithm given below:

- by h is denoted a number such that 2^h divides the rank of g relative to p and such that 2^{h+1} does not divide it,

- h is computed from the Legendre symbol $(g|p)$ and from a number b equal to a 2^t-th primitive root of the unit in CG(p),

- if $(g|p) = -1$ then $h = t$
- if $(g|p) = +1$ with $t = 1$, then $h = 0$
- if $(g|p) = +1$ with $t > 1$, then the key $\langle (p-1+2^t)/2^{t-1}, p \rangle$ is applied to G, a result w is thus obtained:
  - if $w = +g$, then $h = 0$
  - if $w = p-g$, then $h = +1$
  - otherwise, the computation sub-modulus below is applied, by initializing the variable c attributing to it the value b, then iterating the following steps for values of i from t-1 to 2:

step 1: the key $\langle 2^1,p\rangle$ is applied to w/g(modp),

* if the result obtained is equal to +1, go to step 2,

* if the result obtained is equal to -1, the value i is attributed to h and w is replaced by w.c(modp),

step 2: c is replaced by c^2(modp),

the value of h sought is that obtained the last time the application of the key $\langle 2^i,p\rangle$, in accordance with step 1, produced a result equal to -1.

(it may be recalled that

- k, g, p are compatible when h>1 and when k+h>t+1,

- k, g, p are compatible when h=0 or 1, whatever the value of k, or when h>1 and when k+h≤t+1).

(in said algorithm, the Legendre symbol and t have the sense defined in the description).

7. A process according to claim 6 such that to test the second condition, a check is made that at least one set $\{\delta_{i.1} \ldots \delta_{i.f}\}$ is variable or nil,

(δ has the sense defined in the description).

8. A process according to claim 7 such that to test the third condition, a check is made that there is a base number g_i from g_1 to g_m such that the f Legendre symbols $(g_i|p_1)$ to $(g_i|p_f)$ are all equal to +1 or else the f Legendre symbols $(-g_i|p_1)$ to $(-g_i|p_f)$ are all equal to +1.

9. A process according to any one of claims 1 to 8 such that to compute the f.m private components $Q_{i,j}$ of the private values $Q_1, Q_2 \ldots Q_m$ ($Q_{i,j} \equiv Q_i \bmod p_j$), where $G_i \equiv Q_i^v \bmod n$:

- if t = 1 (i.e. if $p_j \equiv 3 \pmod 4$):

- a number s_j is computed such that $s_j \equiv ((p_j+1)/4^k \pmod{(p_j-1)/2}$,
- its key $\langle s_j,p_j\rangle$ is deduced,
- the key $\langle s_j,p_j\rangle$ is applied to G_i,
- we thus have: $w \equiv G_i^{sj} \pmod{p_j}$,

- the two possible values of $Q_{i,j}$ are w, p_j -w,

- if t = 2 (i.e. if $p_j \equiv 5 \pmod 8$):

- a number s_j is computed such that $s_j \equiv ((p_j+3)/8^k \pmod{(p_j-1)/4}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to G_i,
- we thus have: $w \equiv G_i^{sj} \pmod{p_j}$ and $w' \equiv w.z \pmod{p_j}$,
- the four possible values of $Q_{i,j}$ are w, p_j - w, w', p_j - w',

(*in said algorithm z has the sense defined in the description*).

- if t>2 (i.e. if $p_j \equiv 2^t+1 \pmod{2^{t+1}}$) and if h=0 or if h=1,.

- a number s_j is computed such that $s_j \equiv ((p_j-1+2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to G_i,
- we thus have: $w \equiv G_i^{sj} \pmod{p_j}$.
- the $2^{\min(k,t)}$ possible values of $Q_{i,j}$ are equal to the product of w by any one of the $2^{\min(k,t)}$ -th roots of the unit in $CG(p_j)$.

- if t>2 (i.e. if $p_j \equiv 2^t+1 \pmod{2^{t+1}}$) and if h>1 and if $h+k \leq t+1$,

- s_j is computed such that $s_j \equiv ((p_j-1+2^t)/2^{t+1})^{k+h-1} \pmod{(p_j-1)/2^t}$,
- its key $\langle s_j, p_j \rangle$ is deduced,
- the key $\langle s_j, p_j \rangle$ is applied to the 2^{h-1}-th power G_i,
- w is thus obtained
- the 2^k possible values of $Q_{i,j}$ belong to all the products of w by the 2^{k+h-1}-th primitive roots of the unit in $CG(p_j)$.

10. A process according to claim 9 such that to compute the private components $Q_{i,j}$ where $G_i.Q_i^v \equiv 1 \pmod n$, s_j is replaced by $((p_j-1)/2^t) - s_j$ in the key $\langle s_j, p_j \rangle$.

11. A process applying the process, according to any one of the claims 1 to 8, allowing the f prime factors p_1, p_2 … p_f or the m base numbers g_1, g_2 … g_m to be produced:

said process being intended to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of m pairs of private Q_1, Q_2 … Q_m and public G_1, G_2, … G_m values (m being greater than or equal to 1) or parameters derived from them, particularly by means of the private components $Q_{i,j}$:

said process implementing according to the steps hereinafter an entity called a witness;

said witness entity having the f prime factors p_i and/or the parameters of the values of the Chinese remainders of the prime factors; and/or the public modulus n and/or the m private values Q_i and/or the f.m private components $Q_{i,j}$ of the private values Q_i and the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n: each commitment being computed:
  - either by performing operations of the type

$$R \equiv r^v \bmod n$$

where r is a random number such that $0<r<n$,

  - or
  - • by performing operations of the type

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random number associated with the prime number p_i such that $0<r_i<p_i$, each r_i belonging to a collection of random numbers {r_1, r_2,to r_f},

- then by applying the method of Chinese remainders;

- the witness receives one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness computes from each challenge d a response D,

- either by performing operations of the type

$$D \equiv r.Q_1^{d1}.Q_2^{d2} \text{ to } Q_m^{dm} \bmod n$$

- or

- by performing operations of the type:

$$D_i \equiv r_i.Q_{i,1}^{d1}.Q_{i,2}^{d2} \text{ to } Q_{i,m}^{dm} \bmod p_i$$

- then by applying the method of Chinese remainders;

said process being such that there are as many responses D as challenges d and commitments R, each group of numbers R, d, D constituting a triplet denoted {R,d,D}.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
12 avril 2001 (12.04.2001)

PCT

(10) Numéro de publication internationale
WO 01/26278 A1

(51) Classification internationale des brevets[7]: H04L 9/32

(21) Numéro de la demande internationale:
PCT/FR00/02715

(22) Date de dépôt international:
29 septembre 2000 (29.09.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:

99/12465	1 octobre 1999 (01.10.1999)	FR
99/12467	1 octobre 1999 (01.10.1999)	FR
99/12468	1 octobre 1999 (01.10.1999)	FR
00/09644	21 juillet 2000 (21.07.2000)	FR

(71) Déposants *(pour tous les États désignés sauf US)*: **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). **TELEDIFFUSION DE FRANCE** [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75732 Paris Cedex 15 (FR). **MATH RIZK** [BE/BE]; Verte Voie, Boîte 5, B-1348 Louvain-la-Neuve (BE).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)*: **GUILLOU, Louis** [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarre (FR). **QUISQUATER, Jean-Jacques** [BE/BE]; 3, avenue des Canards, B-1640 Rhode Saint Genese (BE).

(74) Mandataire: **VIDON, Patrice**; Le Nobel, 2, allée Antoine Becquerel, Boîte postale 90333, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)*: brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée:
— *Avec rapport de recherche internationale.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** SET OF PARTICULAR KEYS FOR PROVING AUTHENTICITY OF AN ENTITY OR THE INTEGRITY OF A MESSAGE

(54) **Titre:** JEUX DE CLES PARTICULIERS DESTINES A PROUVER L'AUTHENTICITE D'UNE ENTITE OU L'INTEGRITE D'UN MESSAGE

(57) **Abstract:** The invention concerns a set of particular keys designed to prove the authenticity of an entity or the integrity of a message. The proof is established by a set of keys comprising: m (≥1) pairs of private Q_i and public $G_i = g_i^2$ values; a public module n consisting of the product of f(≥2) prime factors; an exponent $v=2^k$ (k > 1), linked by relationships of the type: $G_i . Q_i^v \equiv 1 \mod n$ or $G_i \equiv Q_i^v \mod n$. The set of keys is produced such that: among the m numbers obtained by increasing Q_i or its inverse modulo n to modulo n square, k-1 times rank, at least one of them is different from g_i; among the 2m equations: $x^2 \equiv g_i \mod n$, $x^2 \equiv -g_i \mod n$ at least one of them has solutions in x in the ring of the modulo n integers.

(57) **Abrégé:** La preuve est établie au moyen de jeux de clés comprenant: m (≥ 1) couples de valeurs privées Q_i et publiques $G_i = g_i^2$; un module public n constitué par le produit de f(≥ 2) facteurs premiers un exposant $v=2^k$ (k> > 1), liés par des relations du type: $G_i.Q_i^v = \equiv 1 \mod n$ ou $G_i = \equiv Q_i^v \mod n$. Les jeux de clés sont produits de telle sorte que: parmi les m nombres obtenus en élevant Q_i ou son inverse modulo n au carré modulo n, k-1 fois de rang, au moins l'un d'entre eux est différent de ± g_i parmi les 2m équations: $x^2 g_i \mod n$, $x^2 = -g_i \mod n$, au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n.

WO 01/26278 A1

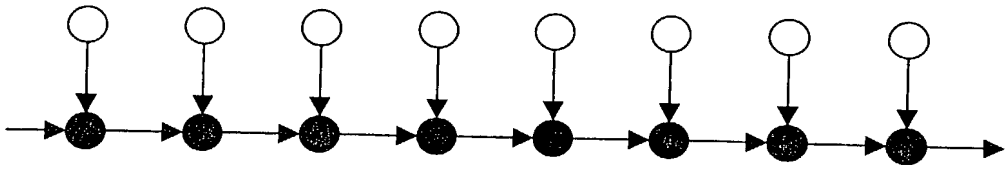


Fig.1A

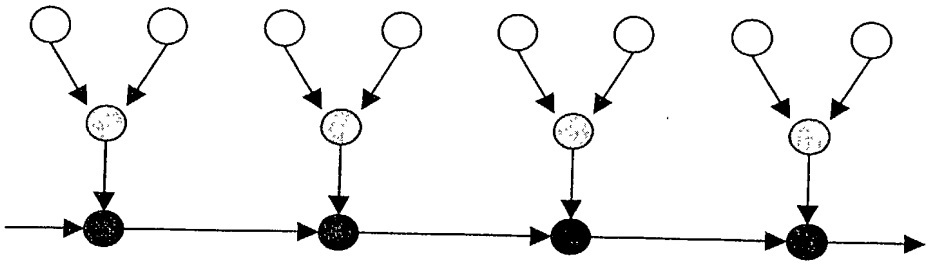


Fig.1B

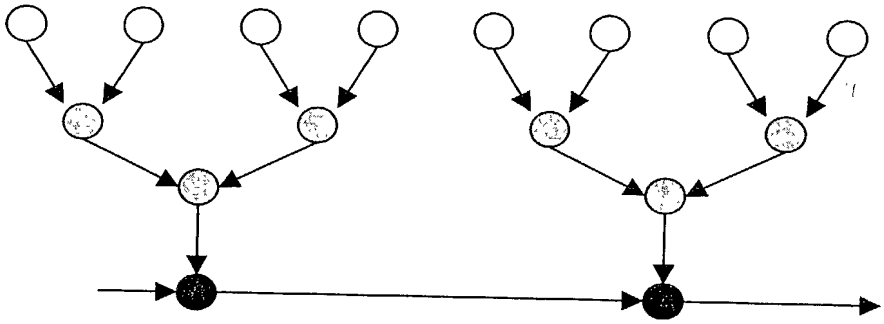


Fig.1C

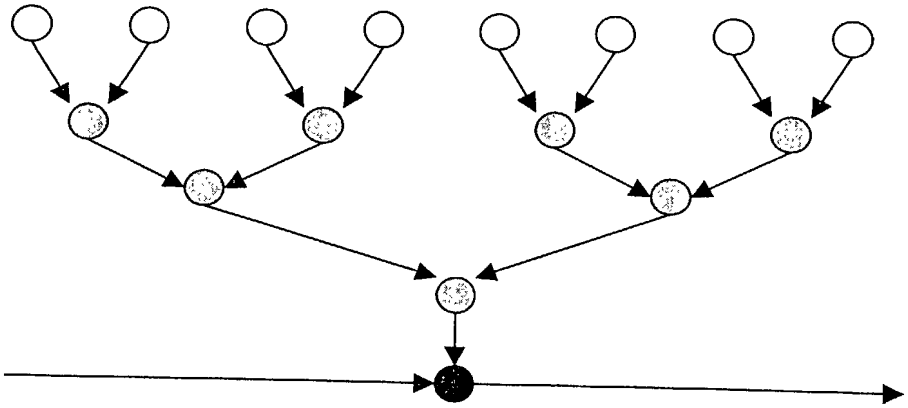


Fig.1D

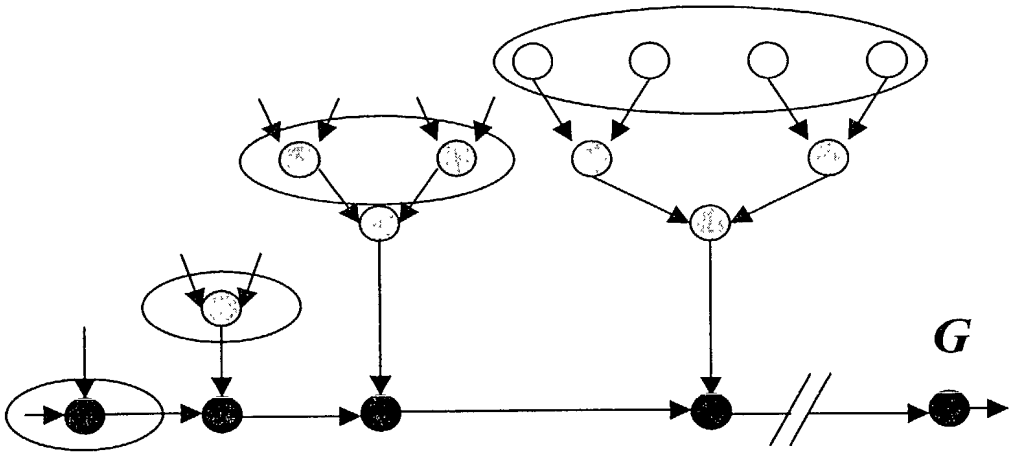


Fig.2A

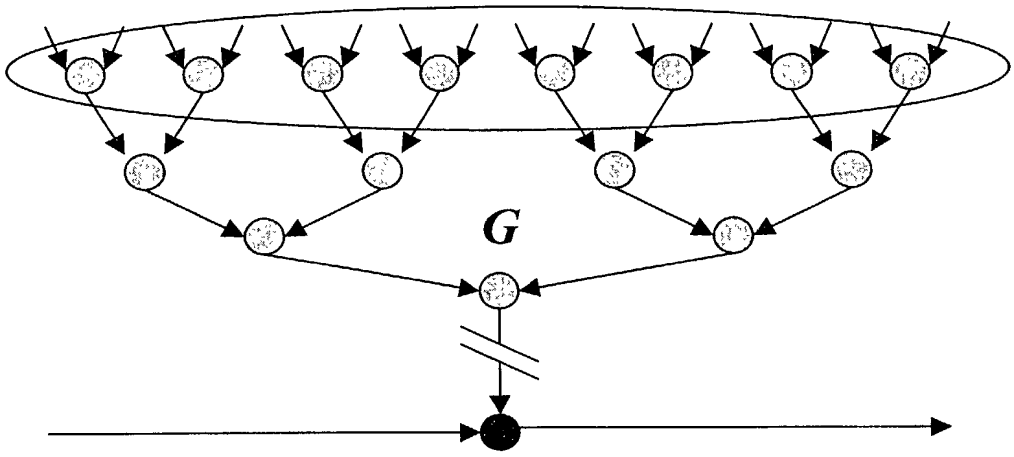


Fig.2B

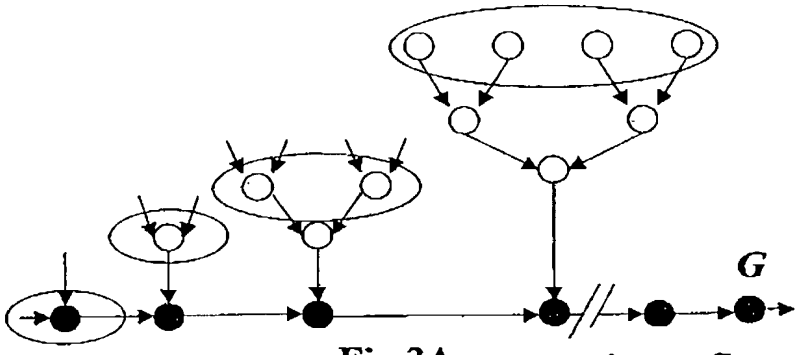


Fig.3A

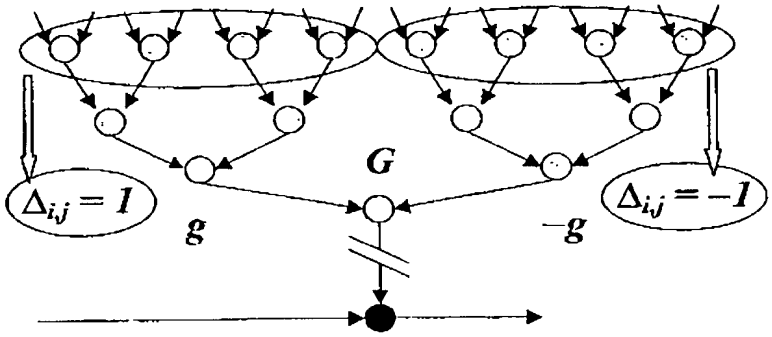


Fig.3B

22 MAI 2002

COMBINED DECLARATION AND POWER OF ATTORNEY IN ORIGINAL APPLICATION

Attorney Docket No.

F40.12-0006

SPECIFICATION AND INVENTORSHIP IDENTIFICATION

As a below named inventor, I declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and joint inventor of the subject matter which is claimed, and for which a patent is sought, on the invention entitled SET OF PARTICULAR KEYS FOR PROVING AUTHENTICITY OF AN ENTITY OR THE INTEGRITY OF A MESSAGE the specification of which,

(check one)
- X is attached hereto.
- X was filed on March 29,2002 as Appln. No. 10/089,646 .
- ___ and was amended on ___.
- X was described and claimed in PCT International Application No. PCT/FR00/02715 filed on 29 September 2000 and as amended under PCT Article 19 on ___.

ACKNOWLEDGEMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is known to me to be material to the patentability of this application in accordance with 37 C.F.R. § 1.56.

PRIORITY CLAIM (35 U.S.C. § 119)

Prior Foreign Application(s)

I claim foreign priority benefits under 35 U.S.C. § 119(a-d) of any foreign application(s) for patent or inventor's certificate listed below, each of which is incorporated by reference in its entirety, , each of which is incorporated by reference in its entirety, and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Number	Country	Day/Month/Year Filed	Priority Claimed
FR99 12465	France	1 October 1999	Yes X No ___
FR99 12467	France	1 October 1999	Yes X No ___
FR99 12468	France	1 October 1999	Yes X No ___
FR00 09644	France	21 July 2000	Yes X No ___

Prior Provisional Application(s)

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States Provisional Application(s) listed below, each of which is incorporated by reference in its entirety:

Number	Day/Month/Year Filed

PRIORITY CLAIM (35 U.S.C. § 120)

I claim the benefit under 35 U.S.C. § 120 of any United States application(s) listed below, each of which is incorporated by reference in its entirety. Insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose to the Patent Office all information known to me to be material to patentability as defined in 37 C.F.R. § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Appln. No.	U.S. Appl. No. (if any under PCT)	Filing Date	Status

DECLARATION

I declare that all statements made herein that are of my own knowledge are true and that all statements that are made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY

I appoint the following attorneys and agents to prosecute the patent application identified above and to transact all business in the Patent and Trademark Office connected therewith, including full power of association, substitution and revocation: Judson K. Champlin, Reg. No. 34,797; Joseph R. Kelly, Reg. No. 34,847; Nickolas E. Westman, Reg. No. 20,147; Steven M. Koehler, Reg. No. 36,188; David D. Brush, Reg. No. 34,557; John D. Veldhuis-Kroeze, Reg. No. 38,354; Deirdre Megley Kvale, Reg. No. 35,612; Theodore M. Magee, Reg. No. 39,758; Christopher R. Christenson, Reg. No. 42,413; Brian D. Kaul 41,885; Robert M. Angus, Reg. No. 24,383; Christopher L. Holt, Reg. No. 45,844; Alan G. Rego, Reg. No. 45,956; and David C. Bohn, Reg. No. 32,015.

I ratify all prior actions taken by Westman, Champlin & Kelly, P.A. or the attorneys and agents mentioned above in connection with the prosecution of the above-mentioned patent application.

DESIGNATION OF CORRESPONDENCE ADDRESS

Please address all correspondence and telephone calls to Robert M. Angus in care of:

WESTMAN, CHAMPLIN & KELLY, P.A.
Suite 1600 - International Centre
900 Second Avenue South
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

Inventor: _____ Date: 22 Mai 2002
(Signature)

Inventor: Louis Guillou
(Printed Name)

Residence: Bourgbarre, France FRX Citizenship: France

P.O. Address: 16, rue de l'Ise, Bourgbarre, France 35230

2-00

Inventor: J.J. Quisquater
(Signature)

Date: 26/04/2002

Inventor: Jean-Jacques Quisquater
(Printed Name)

Residence: Rhode Saint Genese, Belgium BEX Citizenship: Belgium

P.O. Address: 3, avenue des Canards, Rhode Saint Genese, Belgium 1640